HADMÉRNÖK

KATONAI MŰSZAKI TUDOMÁNYOK ONLINE

VII. Évfolyam 1. szám 2012. március

NKE
BUDAPEST

A szerkesztőség elérhetősége:
Nemzeti Közszolgálati Egyetem, 1101. Budapest, Hungária krt. 9-11. A. épület 8. emelet
Postacím: 1581. Budapest Pf.:15.
Telefon: +36-1-432-9048
Fax: +36-1-432-9208
HM: 29-734
e-mail: hadmernok@uni-nke.hu
web: http://hadmernok.hu

Kiadó: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
ISSN 1788-1919

Jelen számban megjelent írások szerzői:

Antal Őrs – Nemzeti Közszolgálati Egyetem

Barbarics Tamás – Budapesti Műszaki és Gazdaságtudományi Egyetem

Bárdos Zoltán pv. alezredes – BM Országos Katasztrófavédelmi Főigazgatóság

Duka Péter – Óbudai Egyetem (MSc hallgató)

Ferencz Bernadette – Paksi Atomerőmű ZRt.

Gávay György mk. főhadnagy – Nemzeti Közszolgálati Egyetem

Dr. habil Grósz Zoltán ny. ezredes – Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet

Horváth Zoltán tü. hadnagy – Nemzeti Közszolgálati Egyetem, doktorandusz

Kovács Ádám – Óbudai Egyetem (MSc hallgató)

Kovács Zoltán – Nemzetbiztonsági Szakszolgálat

Kuris Zoltán – Nemzeti Közszolgálati Egyetem, doktorandusz

Laczik Dóra – Óbudai Egyetem (MSc hallgató)

Dr. Meglécz Katalin – Magyar Honvédség Honvédkórház

Dr. Muha Lajos mk. alezredes – Nemzeti Közszolgálati Egyetem, főiskolai tanár

Dr. Muhoray Árpád ny. tü. vezérőrnagy – Nemzeti Közszolgálati Egyetem Katasztrófavédelmi Intézet

Prof. Dr. Munk Sándor ny. ezredes – Nemzeti Közszolgálati Egyetem, egyetemi tanár

Nagyné Dr. Takács Veronika – Nemzeti Közszolgálati Egyetem, doktorandusz

Nagy Tibor István – Nemzeti Közszolgálati Egyetem, doktorandusz

Németh Balázs

Pápai Tibor – Magyar Honvédség Honvédkórház

Pethő Richárd – Óbudai Egyetem (MSc hallgató)

Petruska Ferenc százados – Nemzeti Közszolgálati Egyetem

Rodriguez, Alejandra Román – Budapesti Műszaki és Gazdaságtudományi Egyetem

Rudolf Ádám – Óbudai Egyetem (MSc hallgató)

Prof. Dr. Szabolcsi Róbert okl. mk. ezredes – Nemzeti Közszolgálati Egyetem, egyetemi tanár

Tajti Balázs – Óbudai Egyetem (MSc hallgató)

Tamási Béla ezredes– MH Vezetési és Doktrinális Központ

Zsákai Róbert

Vágföldi Zoltán

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Kovács Ádám
adam.kovacs.home@gmail.com

ROBBANÓSZER DETEKTÁLÁS ÁLLATOK SEGÍTSÉGÉVEL

Absztrakt

A mai időkben egyre gyakrabban hallani a robbanószerekkel elkövetett merényletekről valamint az elmúlt háborúk által telepített aknák felszámolásának fontosságáról. Éppen ezért a robbanószerek megtalálására, felderítésére újabb és újabb eszközöket találnak ki, de valójában a mesterséges módszerek még gyerekcipőben járnak az állatokkal történő robbanószer felderítéshez képest. Ezen a téren sem szabad megrekedni a robbanószer kereső kutyáknál és éppen ezért szerte a világban próbálkoznak és alkalmaznak sikerrel más állatokat is erre a célra.

Nowadays can be heard more and more about explosive attacks and importance of mine removing. This is the reason why invent new solutions for explosive detection, but in the real word the true is that mechanical modes are worse than explosive detection with animals. There are many animals can detect explosives and scientists try to use them to detect explosives around the world.

Kulcsszavak: *robbanószer detektálás, állat, méh, Pavlov ~ explosive detection, animal, bee, Pavlov*

1. BEVEZETÉS

A tanulmány eredetileg a robbanó anyagok detektálásáról szólt volna és egy kis részét szántam volna az állatokkal való robbanószerkezetek felderítésére. Azonban az anyaggyűjtés és az anyagban való elmélyedés során a robbanószerkezetek ilyen fajta felderítése teljesen magával ragadott. Az ember technikai fejlettsége jelenleg még csak a közelébe sem ér annak, amire a természet képes és talán a jövőben sem éri el azt a hatékonyságot, amit az állatok. A kutatás során olyan új ismereteket szereztem, melyekről eddig fogalmam sem volt. Ezen okokból döntöttem úgy, hogy nagyobb figyelmet érdemel ez a téma és választottam a tanulmányom témájának.

A tanulmány a jelenleg, robbanószerkezet keresésére alkalmazott három állatfajtáról szól. A kutyákról, rágcsálókról és a méhekről. Mindamellett hogy jelenleg a kutyák az elsőszámú robbanószer kereső állatok, mégis a rágcsálókról és méhekről szóló fejezeteknek hasonló terjedelmet szenteltem, mert kuriózumnak tartom és épp ezért olvashatóbb, érdekes témának vélem.

A tanulmány célja:

- Sorra venni a robbanóanyag felderítésben használt állati erőket
- Bemutatni használatukat, kiképzésük módját
- Bemutatni előnyüket és hátrányukat általában és egymással szemben
- Végül, de nem utolsó sorban felhívni a figyelmet az ilyen irányultságú kutatások fontosságára

A tanulmánnyal igyekszem egy kis ízelítőt adni abból, hogy ezen a területen az állatok milyen nagy segítségünkre vannak, és hogy ily módon hány emberéletet mentenek meg. Hányan köszönhetik nekik az életüket és az újabb kutatások milyen mértékben menthetnek meg újabb életeket azoktól az emberektől, akik valamilyen megfontolásból pokolgépekkel próbálnak meg ártani embertársaiknak.

2. KUTYÁS ROBBANÓSZER FELDERÍTÉS

A robbanószerek felderítésére az egyik legjobb és legbiztosabb módszer a robbanószer-kereső kutyák alkalmazása. A kutyák híresek rendkívüli szimatukról és az ember már évszázadok óta használja „legjobb barátjának” orrát. A múltban vadászatra, gombakeresésre vagy épp börtönből szökött gyorsléptű emberek üldözésére használták. Éppen az évszázados használat következtében és a kutyatenyésztők folyamatos munkája révén olyan keresőkutyákat tenyésztettek ki, melyek szaglása már-már hihetetlen mértékeket súrol. A hosszú évek során néhány kutyafajta – némelyiket kimondottan erre a célra tenyésztettek – kimagasló eredményeket mutatott. Ilyen kutyák a vadászat területén például a kopó, agár, retriever, vizsla, véreb, spániel, tacskó és terrier.

2.1. Az alkalmas kutyák

A kutyákat robbanószer keresésére először a 1980-as években kezdték el alkalmazni Afganisztánban.[1] Ezen a szakterületen nem elegendő, hogy egy kutyának jó legyen a szaglása. Kimondottan érzékenynek kell lenniük a robbanószerekre – vegyületeire – és könnyen taníthatóság, fegyelmezettség és barátságosság tulajdonságát kell mutatniuk. Ezek alapján ma kiemelten négy fajta kutyát alkalmaznak. Ezek a kutyák általában labradorok, juhászkutyák, fox terrierek és spánielek.

Vizsgált mozzanatok	Pozitív	Negatív
Viselkedés váratlan zajhatásokra (lövés, feldőlő szék, leeső tárgy)	Nyugodt, hangtalan, figyelmes. Hangforrást megközelíti, vizsgálja.	Ideges, feszült, félénk. Menekül, támadó, agresszív.
Viselkedés fajtársakkal szemben	Nyugodt, kiegyensúlyozott.	Félénk, fokozottan domináns.
Kontaktust teremtő képesség idegen emberekkel szemben.	Bizalmas, kezdeményező.	Ideges, borzolja szőrét.
Viselkedés gépjárművek közelében (motorzaj, légfék)	Nyugodt, hangtalan, vizsgálódó.	Elhúzódás, kiútkeresés, remegés, támadás, fejkapkodás.
Viselkedés mozgó járműben	Nyugodt, hangtalan, érdeklődő	Remegés, fejkapkodás.
Viselkedés magasban és mélyben	Nyugodt, készséggel elfogadja az emberi segítséget.	Remeg, nyáladzik. Emberi segítségre támad.

1. táblázat. A kutya pozitív és negatív tulajdonságai az alkalmasság szempontjából.
Forrás: http://www.nolandmines.com/using animals as detectors.htm (2011-04-21)

2.2. A kutya orrának felépítése, működése

A kutya szaglószerve lágy szövetekből, csontokból, idegekből és az agy egyes részeiből áll. A lágy szövetek és csontocskák alkotják azt az üreget, ahová a levegő részecskéi áramlanak. Ebben az üregben sorakoznak fel az illatreceptor-sejtek, amelyek a szaglószervi idegekhez, azok pedig a kutya szaglószervi agylebenyéhez csatlakoznak.

A kutyák nyálkahártyája nagy redőkből áll, melyek több mint 200 millió illatreceptort foglalnak magukba kisebb helyen, mint az emberé, mely csak 5 millióval rendelkezik. Az ő szaglószervi gumóik négyszer nagyobbak, mint a mieink. Mindezek mellett vannak fajták, melyeket szagló munkára tenyésztettek. A hosszabb orrú kutyáknak sokkal több illatreceptora van. A kutyák szagláskor másik útvonalon áramoltatják a levegőt, mint normál légzésnél. Az orrüregük felső részét is igénybe veszik ilyenkor, mert így a levegő több receptorral képes érintkezni.[1]

2.3. A kutya kiképzése

A kiképzési folyamat az egyedek kiválasztásával kezdődik. A legtöbb helyen maga a felhasználó szervezet tenyészti a kutyákat, szigorúan alkalmassági alapon. Az almokból különböző vizsgálatokkal és tesztekkel választják ki a speciális feladatokra alkalmas kutyákat. A kiválasztás igen szigorú paraméterekkel zajlik, hiszen ettől emberi életek függhetnek.[2]

Magyarországon a legelterjedtebb keresőkutya a németjuhász. A választás azért erre a fajtára esett, mert nagy a terhelhetősége és megjelenése az egész világon egyértelművé teszi, hogy munkakutyával van dolga az embernek.[2]

A keresőkutyák kiképzése – legyen szó drogról vagy robbanószerről – mindig ugyan úgy zajlik. A legfontosabb, hogy játékos természetű legyen, mert ez a kulcsa annak, hogy jó kereső legyen belőle. A ebnek a robbanószer megtalálása csak közvetett célja. A kiképzés során kedvenc játékát használják a betanításhoz. Ezt a játékot hívják apporttárgynak. A tanulás során először az apporttárgyát kell megkeresnie, melyet elrejtenek előle. Később a Pavlovi reflex segítségével fog a kutya robbanószert keresni. Ez úgy zajlik, hogy a tárgyat összefüggésbe hozzák a keresett anyag szagával, majd az apporttárgyat kiemelik a kutya látómezejéből és az állat automatikusan keresni fogja. Azonban a kutya a játékkal összefüggésbe hozott szagot fogja keresni és végül megtalálni. Amikor megtalálta a kiképző által keresett robbanószert, megkapja az apporttárgyat. Az, hogy az eb megkapja játékát valamint, hogy simogatással megerősítsék abban, hogy jól dolgozott nagyon fontos a pozitív megerősítés szempontjából. A kiképzés utolsó szakaszában különbözőképpen kialakított helységdíszletek, majd később igazi épületek viszonyai között kell megkeresnie az elrejtett robbanóanyagot. Amennyiben itt is jól teljesít, elmondható, hogy kiképzése sikeres volt. Természetesen ezzel nem ér véget a képzés. Folyamatos törődést és képzést igényel azért, hogy ne felejtse el vagy épp, hogy újabb anyagok felderítésére legyen alkalmas.

Az ebek a kiképzés során 10 dkg és 10 kg mennyiség közötti robbanóanyagok felderítését sajátítják el. Egy átlagos keresőkutya a célponttól 2-3 méterre érzi meg a keresendő tárgyat, azonban ezt befolyásolhatja orrának érzékenysége vagy akár a légáramlat is. Fontos, hogy a drogkereső kutyákkal ellentétben a robbanószer keresésére kiképzett állat nem adhat hangjelzést, mert nem lehet tudni, hogy a detonáció milyen hatásra következik be. Ezért azzal jeleznek, hogy leülnek vagy lefekszenek a céltárgy elé, persze ez sem mindegy hisz ennek is jelentősége van. Ha ül, akkor az orrszintje felett, ha fekszik, alatta található a keresett robbanóanyag.

Alkalmazott robbanóanyag	**Felhasználási eszköz**
TNT (Trinitro-toluol), présel	TNT 75g-os; TNT 400 g-os; FRT 2,5; FRT 5
Semtex-H (Hexogén Nitropenta és Flegmatizátor)	Semtex-H; SZZ-IE (szalagtöltet)
Paxit (normál paxit, paxit-3, paxit-4)	Normál paxit; paxit-3; paxit-4
Flegmatizált Hexogén (A-IX-1)	PG-7-M kumulatív gránát
Flegmatizált Hexogén Alumíniummal (A-IX-2) 1	125 mm-es OF-26 repesz-romboló gránát
Öntött TNT Hexogén Alumíniummal és Flegmatizáltorral (TGAF-5)	122 mm M-21 OF sorozatvető rakéta (9M22U) harcirész
TNT és Dinitro-napftalin (TD-42 vagy TD 50)	82 mm-es O-832DU repesz aknagránát
TNT és Ammónium-nitrát ötvözete (amatol AT-40 vagy AT-90, AT-80)	82 mm-es O-832DU repesz aknagránát
Fekete „füstös lőpor”	Gyári mintából
„ Gyérfüstű” piroxilines és glicerines lőporok	Gyári mintából

2. táblázat. A Magyar Honvédség keretein belül alkalmazott szagminták.

2.4. Előnyök, hátrányok

A kutyás keresés előnyei:

- A kutyák orra rendkívül érzékeny. Az ember technikában még csak meg sem tudja közelíteni ezt az érzékenységet. A kutyák azt is megérzik, ha valaki csak érintkezett az anyaggal nem feltétlenül kell tisztán nagy mennyiségben ott lennie. Gondoljunk csak arra, hogy annak ellenre, hogy bezacskózzák az anyagot, majd lemossák a zacskót, a kutya rátalál a keresett anyagra.
- Kis területen gyors átvizsgálási lehetőséget biztosít.
- Nem utolsó sorban pedig elrettentő, preventív hatása is van.

Hátrányai:

- Túlérzékenység. A kutyáknak, ha túl gyakran kell kismennyiségű robbanóanyagot keresnie, akkor bizonytalanná válnak és megpróbálják más szaganyagokkal kipótolni a kereséshez szükséges illatanyagot. Ez ahhoz vezet, hogy egy idő után más szagokkal fogják azonosítani a robbanóanyagot.
- A kutyák orra telítődhet a szaggal. Ez a jelenség ahhoz hasonlít, mint amikor az ember egy illatosítót vesz a kocsijába, akkor azt egy idő után nem érzi, mert hozzászokik, azonban aki frissen ül a kocsiba annak új az illat és megérzi. Ez azzal jár, hogy bizonyos időnként a kutyáknak pihenniük kell.

3. RÁGCSÁLÓKKAL VALÓ ROBBANÓSZER FELDERÍTÉS

A világon szinte mindenütt elterjedt a kutyatartás, azonban sok esetben az őshonos kutyafajta nem kimondottan alkalmas keresésre. Ilyen helyeken is szükség lehet a robbanóanyag kereső állatokra. Bizonyos országokban ezért a rágcsálókat részesítik előnyben. Nem titok, hogy egyes rágcsálóknak rendkívül kifinomult szaglása van. A háborúk alatt letelepített több százezer vagy akár millió akna felderítése céljából használnak főként rágcsálókat.

3.1. APOPO program

Belgiumban az APOPO (Anti-Personnel Landmines Detection Product Development – Gyalogsági Aknák Felderítésére irányuló Termékfejlesztés) program keretin belül tanítanak rágcsálókat aknák felderítésére. A programot a belga Bart Weetjens kezdte azzal a céllal, hogy alacsony technikai színvonalon képesek legyenek aknák felderítésére. A program keretein belül Gambiai erszényes patkány – 1.ábra –használnak.

1. ábra. Gambiai erszényes patkány
Forrás: www.apopo.org képgalériájából

A kísérleteik igazolták, hogy a patkányokkal hosszútávon érdemes foglalkozni. Ráadásul a kísérletek azt is bizonyították, hogy a patkányok az aknákon kívül még a tuberkulózist is „diagnosztizálni" tudják. Az APOPO program keretein belül elnevezték ezeket a patkányokat HeroRAT-nek (HősPatkány), mivel az aknák felderítésével életeket mentenek, és mindezt hatékonyabban és olcsóbban teszik, mint bármely más módszer.

Az, hogy a rágcsálókat aknafelderítésre használják csak a kezdet. Természetesen semmi sem zárja ki annak a lehetőségét, hogy a patkányok ne csak aknákat, hanem terrorista célokra készített robbanószerkezeteket is megtaláljanak.

2. ábra. APOPO Mozambikban
Forrás: www.apopo.org

Jelenleg a HősPatkányok Mozambikban – 2. ábra – aktívan tevékenykednek. Lehetővé tették, hogy több mint 1000 család visszatérhessen lakhelyére és további 10000 mozambiki számára az összeköttetést más településekkel azáltal, hogy megtisztították az utakat. Ha minden jól megy, a tervek szerint 2013-ra a teljes területet akna mentesítik.

3.2. Rágcsálók előnyei

Mi szól a rágcsálók mellett?[3]

- A legtöbb helyen a patkányok őshonosak, jobban bírják a helyi klímát és a helyi betegségeknek is jobban ellenállnak, mint a kutyák. Sokkal könnyebben alkalmazkodnak a környezethez.
- Kiképzésük lényegesen kevesebb időt vesz igénybe.
- Tartásuk, tenyésztésük költségkímélőbb és egyszerűbb.

- Felnevelésük gyors és kevés erőforrást igényel.
- A képzés ideje és a patkány életidejének aránya sokkal kedvezőbb.
- A patkányok nem ragaszkodnak egy gazdához.
- Méretüknek köszönhetően kis eldugott helyekre is befférnek.
- Súlyuk miatt a robbanószerkezetet (taposóaknát) nem hozzák működésbe.
- Méretükből, könnyű szaporításukból és gyors kiképzésükből adódóan nagy mennyiségben vihetők egy adott területre.
- Kevésbé fáradékonyak szaglás területén, de ha el is fáradnának könnyebb másik patkánnyal helyettesíteni őket.

Mi szól ellenük?

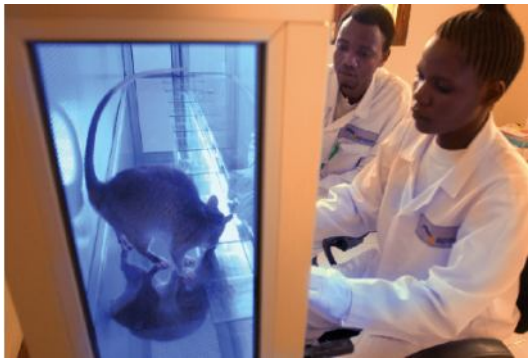
- A kutyákkal ellentétben a rágcsálókról nem igazán mondható el, hogy elrettentő hatásuk van. Egy kutya látványa a preventív védelmet erősíti.
- Bár szaglásuk vetekszik, de az nem kérdéses, hogy a kutya intelligenciája nagyobb és így több feladatot is elláthat (pl.: kutyás őr=védelem), melyek olyan területeken, mint a határátkelők, repterek elengedhetetlenek.

3.3. Kiképzésük

A patkányok kiképzése – 3. ábra – 8–12 hónapot vesz igénybe. A patkányok is a Pavlovi reflex útján tanulják meg a robbanószer keresését. Az állatokat először egy kis „klikk” hang kíséretében etetik, hogy megtanulják összefüggésbe hozni az ételt a hanggal. Később ezt a hangot hallatják a robbanószer szagának érzékelésekor és ezután kapnak élelmet. Ezzel a módszerrel előbb-utóbb megtanulják, hogy a robbanószer szaga ételt jelent és így azt fogják keresni.[4]

3.4. Hasonló kutatások

Az APOPO kísérletein felbuzdulva már Kolumbiában is folynak kísérletek robbanóanyag kereső patkányok tenyésztésére. Az INVESTUD (*The Interdisciplinary Research Group*) fehér kísérleti egeret – 3. ábra – képez ki erre a célra.[5]



3. ábra. Patkányok képzése
Forrás: www.apopo.org

Két fő okból alkalmazzák a fehéregeret a gambiai erszényes patkány helyett:[5]

- A fehéregér könnyebb és kisebb méretekkel rendelkezik (1500 g helyett csak 450 g)
- A fehéregér a világ bármely pontján könnyen tenyészthető, hisz kísérleti célokra használják világszerte.

4. ábra. Kísérletekhez használt fehéregér

Mint láthattuk a rágcsálókkal való robbanószer keresés már nem csak kísérleti stádiumban van, hanem javában zajlik. Tulajdonképpen semmi sincs, ami útjában állna, hogy ők végezzék el teljes mértékben a kutyák dolgát.

4. MÉHEKKEL VALÓ ROBBANÓSZER FELDERÍTÉS

Az emberek és méhek régre nyúló közös múlttal rendelkeznek. Ókori spanyol barlangrajzok egy mézet begyűjtő nőt ábrázolnak. Az egyiptomiak méheket szállítottak fel és le a Níluson. Napjainkban az Afganisztán területeiről származó mézelő méhek (Apis mellifera) terjedtek el az egész világon az Arktisz és Antarktisz kivételével mindenütt. Minden közösségben és országban a méheket a mézért, viaszért és a termőföldek beporzásáért tartották.[6]

Valószínűleg mindenki hallott már arról, hogy robbanóanyagok után kutyákkal kutatnak, még talán a rágcsálókról is. Azonban felmerülhet a kérdés, hogy ha az emlősök képesek rá akkor esetleg más állatfajok is. A rovarok sokkal régebb óta élnek bolygónkon, és még ha első gondolatunk nem is az róluk, hogy sok olyan képességgel rendelkeznek, melyekről az emlősök még csak nem is álmodhatnak, mégis el kell ismerni, hogy bizonyos tulajdonságaikkal felénk magasodnak. A méhek a közelmúltban jelentős figyelmet kaptak annak köszönhetően, hogy képesek a robbanóanyagok, aknák és UXO-k (fel nem robbant bombák) skálájának nagy részét érzékelni.

4.1. A kutatás kezdete

A modern háborúk egyik következménye, hogy rengeteg elaknásított terület maradt fenn utánuk, világszerte. A dél-szláv háborúk alatt a volt Jugoszlávia területén hatalmas mennyiségű akna maradt telepítve, melyek felderítése lehetséges ugyan, de olyan költséges hogy mindmáig elvégezetlen munka maradt. Ezt az állapotot akarta megszüntetni a horvát professzor Nikola Kezic.[7] Kezic aknakeresésre akarta betanítani a méheket. Kutatásai nyomán indult el 1999-ben az Egyesült Államokban a kísérlet, miszerint méheket tanítanak be robbanószer keresésre. Azonban nem csak az USA-ban próbálták ezt a módszert. 2004-ben a Charles de Gaulle párizsi repülőtéren 15-18 hónapig treníroztak méheket robbanószer keresés céljából.

4.2. A kutatások mai időkben

Néhány éve a kutatók a Montanai Egyetemen olyan képességekkel ruházták fel a méheket, hogy érdekeltek legyenek bizonyos illatok megérzésében. A méheknek rendkívüli érzékenységű szaglásuk van és betaníthatók robbanóanyagok, bombák és aknák megtalálására. Hasonló hatékonysággal bírnak más kémiai anyagok terén is, mint például a

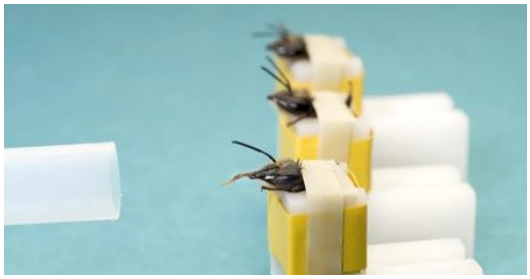
drogok vagy bomló tetemek.[8] A New York Times sikerről számolt be, amikor közzé tette, hogy a betanított méhek 99%-os sikerrel megtalálták az elrejtett robbanószereket.[9]

Az utóbbi időkben mindinkább növekvő terrorista fenyegetettség ezt a kutatást is elősegítette. Új-Mexikóban található Los Alamos Nemzeti Laboratórium kutatói biztosak abban, hogy sikerült nekik méheket betanítani robbanóanyag keresésére a szívókájuk segítségével, amivel egyébként a méhek táplálkoznak. Már csak egy hordozható kaptárt kell kifejlesztenie a rovarok szállítására, valamint ki kell dolgoznia a tematikát a "felhasználók" oktatásához.[10] A Department of Defense Advanced Research Projects Agency's (DARPA's) 1,5 millió dollárral támogatta a Laboratórium kutatásait. A kutatás vezetője Dr. Timothy Haarmann biológus.[8]

További, méhekkel kapcsolatos kísérletekkel a Texas állambeli San Antonio város Délnyugati Kutató Intézete (Southern Research Institute) lett megbízva a DARPA's részéről, kooperálva a Sandia Nemzeti Laboratóriummal (SNL) és a Légierő Kutató Laboratóriumával (AFRL).

4.3. Folyamat működése és kiképzésük

A méhek kiképzése hasonló a kutyákéhoz. Étellel jutalmazzák őket, mely jutalom hatására a keresett anyagról mindig az ételre fognak asszociálni. A betanítás a következőképp történik. Kiválasztanak néhány méhet a kaptárból, melyek nyelvéhez a keresendő robbanóanyagnak megfelelő szagminta kis mennyiségét érintik – 5. ábra – majd ezt követően jutalomképp cukros vizet adnak a méheknek.[9]



5. ábra. Méhek betanítása
Forrás: http://www.geekologie.com

Tulajdonképpen Ivan Petrovics Pavlov reflex kísérletei alapján működik az eljárás. Nagy előnye, hogy ez a betanítás 10 percet vesz csak igénybe és nem szükséges egyesével betanítani a kaptár összes méhét, elég egy-kettőt, ugyanis a betanított egyed hazarepülve megossza az információt – a keresendő illatot – társaival és együtt erednek a robbanóanyag nyomába. A mézelő méhek testén elágazó szőröcskék fejlődtek ki, melyek statikus elektromos töltöttsége rendkívül jó hatásfokkal gyűjti össze a kémiai és biológiai részecskéket, beleértve a szennyeződéseket, hadászati- és robbanóanyagokat.[6] Kifinomult szaglásuknak köszönhetően a dinamittól a C-4-ig bármilyen robbanószert megtalálnak.[10]

A kutatók megfigyelték, hogy a méhek „szaglása" rendkívül finoman hangolt és akár 10 pptr ($10{:}10^{12}$, 1egység/billióegység) arányban homokkal kevert Di-Nitro-Toluol kimutatására is képesek voltak. Rendszerint 50-80 pptr arány felderítése volt megfigyelhető. Ez az érték nedves környezetben 30 pptr értékre nőtt.[6]

4.4. Előnyeik, hátrányaik

További előnye a méheknek azon kívül, hogy „szaglásuk" vetekedik a kutyáéval az, hogy képesek egész álló nap végezni a munkájukat (kivéve esős időben és éjjel). Valamint sokkal gyorsabbak, csapatostól jóval nagyobb területeket képesek bejárni – berepülni – mint a kutyák.

Természetesen előnyeik mellett hátrányaik is vannak, hisz ha nem lennének, akkor úgy gondolom már mindenhol „repkedő tűzszerészeket” látnánk.

Ezek a hátrányok a következők:

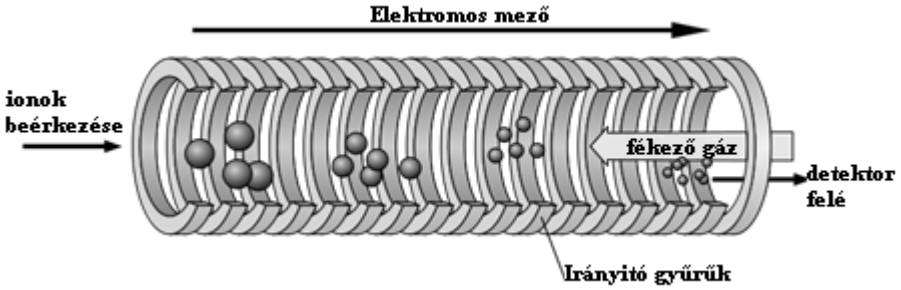
- Éjjel és esős időben nem használhatók, mert a méhek nem repülnek ilyen körülmények között
- Emberekkel zsúfolt helyen nem igazán látják őket szívesen

Mindezek és a kritikák ellenére a kísérletek pozitív visszajelzései bizakodásra adnak okot. Talán már nincs is olyan messze az idő mikor a robbanószerek felkutatása gyerekjáték lesz a méhek közreműködésével.

5. MECHANIKUS ILLATFELDERÍTÉS

Fontosnak tartottam – mindamellett hogy sok szépet és jót leírok az állatok robbanószer keresési képességéről – megemlíteni, hogy hol is tart jelenleg a technika a természet által oly fantasztikusan megalkotott szaglás, mint érzékelés leutánzásában.

A leggyakoribb alkalmazása a mechanikus illatdetektálásnak látható az Egyesült Államok repterein. Ez nem más, mint az IMS (Ion Mobility Spectrometry – ion mobilitás spektrometria). Hasonló a tömegspektrometriához, ahol a molekulákat ionizáljuk, majd vákuum alatt egy elektromos mezőbe irányítjuk és a mérő részen a becsapódásból számoljuk a tömegét, azzal a különbséggel, hogy az IMS légköri nyomás alatt dolgozik és a molekula sebességét vizsgálja. Attól függően, hogy meddig tart egy ionnak keresztülhaladni az IMS – adott hosszúságú – elektromos mezején, meg lehet állapítani az ion méretét, ugyanis az ion átmérője minél nagyobb, annál több légköri részecskével ütközik és ez által az befolyással van a sebességére. Ebből a sebességből lehet megállapítani az ion méretét. Minél lassabb egy molekula annál nagyobb.[11]



6. ábra. IMS működése.[12]
Forrás: http://en.wikipedia.org/wiki/Explosive_detection#Mechanical_scent_detection; (2011. 04. 21.)

Ez a technika, mint ahogyan más „szaglás leutánzó” szerkezetek is jól működnek, alapos kutatás van mögötte mégsem vehetik fel a versenyt az állatvilágban kialakult szaglószervekkel. Mindezek ellenére úgy gondolom, az ember eljuthat arra a szintre, hogy saját maga egy olyan berendezést kreáljon, mely helyettesíti az állatokat ebben a feladatban, azonban az én elképzeléseim szerint mindezt szervetlen anyagból nem leszünk képesek elkészíteni.

6. ÖSSZEFOGLALÁS

A dolgozatom segítségével talán világossá vált, hogy az emberek által létrehozott szerkezetek jelenleg még csak gyerekcipőben járnak ahhoz képest, amire az állatokkal való együttműködés képes. A dolgozatban bemutattam három állatfajtát, melyek segítségére lehetnek az embernek a robbanószerkezetek hatékonyabb felderítésében. Bemutattam, hogy bár jelenleg a kutyák dominálnak és őket preferálják az emberek más állatokkal szemben,

azok számára, akik elolvasták ezt a dolgozatot lehetőség nyílt, hogy meglássák a rágcsálókban és méhekben rejlő lehetőségeket.

Ezt a meglátható lehetőséget támasztottam alá azzal, hogy sorra vettem azokat az állatokat, melyek segítségünkre lehetnek ebben a munkában, bemutattam használatukat, kiképzésüket, előnyüket, hátrányukat. Megemlítettem pár kutatást, mely ezzel foglalkozik. Bemutattam őket, mellyel remélhetőleg felhívtam a figyelmet ezen kutatások fontosságára.

Egy kis ízelítőt adtam abból, hogy ezen a területen az állatok milyen nagy segítségünkre vannak, és hogy emberéletek múlnak az ő munkájukon.

Remélem az olvasónak is legalább annyira felkelti érdeklődését, mint nekem és meglátja a fantáziát ezekben a lehetőségekben.

Felhasznált irodalom

[1] Joy Buttler, The tracking dog's nose, http://www.suite101.com/content/the-tracking-dogs-nose-a51486; (2011. 04. 21.)

[2] http://www.szrfk.hu/rtk/kulonszamok/2009_cikkek/Daruka_Norbert.pdf; (2011. 04. 21.)

[3] Wikipedia, http://en.wikipedia.org/wiki/APOPO; (2011. 04. 21.)

[4] Apopo, http://www.apopo.org/mine_detection.php; (2011. 04. 21.)

[5] Luisa Fernando Mendez Pardo és Andres M. Peres-Acosta, The Journal, Research in Columbia on explosive detection by rats, http://maic.jmu.edu/journal/13.3/notes/pardo_etal/pardo_etal.htm; (2011. 04. 21.)

[6] Honey Bees and landmine detection, http://learekow.blogspot.com/2008/12/honey-bees-and-landmine-detection.html; (2011. 04. 21.)

[7] CTV news, Bees are the new buzz in explosives detection, http://www.ctv.ca/CTVNews/SciTech/20061209/bees_explosives_061209/; (2011. 04. 21.)

[8] Sulinet, http://www.sulinet.hu/tart/fncikk/Kjbd/0/7368/robbano_mehek.htm; (2011. 04. 21.)

[9] Háború Művészete, Robbanóanyag-kereső méhek, http://www.haborumuveszete.hu/rovatok/hirek/mehek_061128/?print; (2011. 04. 21.)

[10] Hill and Honey, http://hillendhoney.blogspot.com/2011/01/explosive-detector-bees-check-this-out.html; (2011. 04. 21.)

[11] Wikipedia, http://en.wikipedia.org/wiki/Explosive_detection#Mechanical_scent_detection; (2011. 04. 21.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Laczik Dóra
laczik.dora@gmail.com

HAMIS TŰZJELZÉS KISZŰRÉSÉNEK ELVI ÉS GYAKORLATI LEHETŐSÉGE A TŰZVÉDELEMBEN

Absztrakt

A cikk célja, hogy bemutassa azokat a tűzvédelemben használatos eszközöket, amelyek segítik a tűz mihamarabbi észlelését. A szerző fontosnak tartja, hogy a felesleges tűzoltósági vonulások lecsökkenjenek, hiszen amikor az egységek kivonulnak egy téves riasztáshoz és van rá esély, hogy az idő alatt befut egy éles riasztás, ahová így az egységek kiérkezésének ideje megnő. A téma kifejtés során kitér a téves jelzések keletkezésének az okaira, valamint azok kiküszöbölésének a módjaira.

The article aims to illustrate the use of fire protection devices, which help the early detection of fire. The author believes that the extra runs are reduced to the fire department, because when the units pull out of a false alarm and there's a chance that the time you run into a sharp alarm, so the units where the arrival time increases. The topic of discussion deals with the generation of false signals to the causes and ways to eliminate them.

Kulcsszavak: *téves jelzés, tűzjelzés ~ false signal, fire alarm*

1. BEVEZETÉS

A nem kívánt tűz megfékezése ma már minden elemében tudatos tevékenységen alapszik, az ártó tűz mielőbbi elfojtásának gyakorlati szükségletéből fakad, a tudomány és a technikai fejlődés legújabb eredményeire épül, tudományos ismeretek alapján kidolgozott technológiát és ennek megfelelő gyakorlatot, egyre eredményesebb küzdelmet jelent. A világban minden társadalom számára sebezhetőséget, az élet és a tulajdon közvetlen veszélyeztetettségét jelenti a tűz, annak ellenére, hogy különböző tűzoltási technológiák és tűzvédelmi figyelmeztetések vannak. Az aktív és passzív tűzvédelmi megoldások – értem ez alatt az épületszerkezetektől a beépíthető oltórendszerekig valamennyi tűzvédelmi rendszert – valamint a hivatásos, a létesítményi és az önkéntes tűzoltóságok egyre jobb és jobb technikai felszereltségét, a tűz és a hozzá kapcsolódó káros hatásai mind a mai napig jelentős hányadát képviselik a káreseményeknek. A tűzmegelőzés egy olyan alapvető szakterület, amelynek célja elsősorban az élet megóvása, a biztonságos kimenekülés feltételeinek megteremtése és nem utolsó sorban az anyagi javak védelme aktív és passzív tűzvédelmi berendezések létesítésével, egyedi használati előírások megtételével. Minden állampolgárnak kötelessége a tűz elleni védekezés. Mindenkinek meg kell ismernie, és be kell tartania a tűzmegelőzési szabályokat, a tűz- és káresetek jelzésével, továbbá a tűz oltásával és a műszaki mentéssel kapcsolatos kötelezettségeket. Ellenszolgáltatás nélkül segítséget kell nyújtania minden állampolgárnak a rendelkezésükre álló híradási, vagy közlekedési eszközökkel a tűzjelzéshez, a segítségkéréshez és a visszajelzéshez. Gazdasági és egyéni érdekek fűződnek ahhoz, hogy mihamarabbi információt szerezzünk a nem kívánt tűzről, tehát a lehető legkorábban észlelni kell. Ezt már a régi időkben is fontosnak tartották. Döntő befolyással van a tűz keletkezése és az oltás megkezdése közt eltelt idő a tűz kiterjedésére, kifejlődésére illetve a kárérték nagyságára. A tűz eredményes oltását befolyásolják a rendelkezésre álló információk, az információk továbbításának módja, gyorsasága és a tűzoltásban résztvevők kommunikációja.

A szerző választása azért esett erre a témára, mert fontosnak tartja azt, hogy az akaratlanul vagy akarattal keletkezett tüzeket még a kezdő stádiumban észleljék, és mielőbb jelezzék a tűzoltóság felé, hiszen minden perc számít. Fontosnak tartja, hogy a téves jelzések száma minimalizálódjon és így csökkenjenek a felesleges tűzoltósági vonulások, az áramtalanítások, az épület kiürítése, egyes tevékenységek leállítása és az ezekből adódó tetemes anyagi károk vagy éppen a rendszer működésképtelensége, vészhelyzetben, egy fel nem derített hiba miatt.

2. A TŰZ ÉS ÉRZÉLEKHETŐ JELLEMZŐI

A tűz maga kémiai és fizikai folyamatok sokasága, az éghető anyag oxidálódik, így a rendszer anyagi és energiaállapota megváltozik. Ezen változások révén égéstermékek keletkeznek, valamint hő szabadul fel és ezt a folyamatot fényjelenség is kísérheti. A detektálás szempontjából a tűzvédelemben energiaváltozás esetén a hő és a fény (láng) képződése az, amit az automatikus jelzésadók érzékelni tudnak, valamint az anyagi jellemzők változásánál a füst és gázképződés. Ahhoz, hogy egy automatikus tűzjelző rendszer a tüzet minél korábban jelezni tudja, olyan jellemzőket kell figyelnie, melyek egyértelműen definiálják a tűz jelenlétét. Következtetésképpen levonható, hogy a tűzjelző rendszerek érzékelő eszközeinek működése a tűzjellemzők mérésén alapul.

Ezek az úgynevezett tűzjellemzők két csoportba oszthatók:

energiaváltozás

a) fény (láng): infravörös és ultraibolya sugárzás.

b) hő: hővezetés, hőáramlás.

c) nyomás: nyomáshullám, hang.

anyagi jellemzők változása

a) gázok: CO, CO2, HCN.

b) füst: szilárd aeroszolok, bomlástermékek, korom, gőz.

3. EMBERI TÉNYEZŐK, TECHNIKAI RENDSZEREK FEJLESZTÉSE

3.1. Tűzriasztás személyes megfigyeléssel

A tűz elleni küzdelem fejlődésének történetében már igen korán felleljük a tűzjelzésre és a riasztásra való igényt. Ahhoz, hogy a tüzet időben észleljék, folyamatos és megbízható őrködésre van szükség. A figyelők feladata, hogy az egész települést és a hozzá tartozó területeket figyeljék, ha tűz van az egész lakosságot riasszák. Az őrök fizetést kaptak, és ha mulasztást követtek el, akkor felelősségre vonták őket, illetve szankciót kaphatott az egyén. A feladatot ellátta: éjjeli őr, éjjeli őrjárat, toronyőr, a tűzőrségeknél a figyelőőr. Nappali őrjáratokat minősített helyzetekben alkalmaztak, ilyenek voltak az aratások, búcsúk és a vásárok.

Pannónia székhelyén, Aquincumban ásatások során feltárták egy torony maradványait, amely valószínűsíthetően az egykori tűzoltó székházhoz tartozhatott. A toronyban folyamatosan megfigyelők szolgáltak, tűz esetén hangjelzés útján adták tudomására a tűzőrségnek és a polgároknak. Voltak olyan esetek, amikor a toronyőr nehezebben derítette fel a tüzet, mint a járőr. Megoldást jelentett, hogy egyszerre legyen járőr és toronyőr is, akik között kapcsolat volt. Ha jók voltak a látási viszonyok éjjel, akkor fényjeleket használtak, hangjelekkel kiegészítve. Ha rosszak voltak a látási viszonyok, akkor éjjel és nappal is hangjelekkel kommunikáltak (kolomp, csengő, fém ütögetése, harsona, trombita). A tűzőrség tagjai tűz esetén a tűzoltószerekkel a helyszínre vonultak, hang és más jelek kíséretében. Az emberek közötti kapcsolat főképp az élőszó volt, de egyezményes vizuális és akusztikus jeleket is alkalmaztak az oltás közben és egyéb feladatok ellátásakor.[1]

Alapvető követelmény volt, hogy a tűz keletkezését a lehető leggyorsabban hírül adják. A hagyományos vagy az elektronikai eszközökkel továbbított tűzhír befuthat pl.: egy tűzoltó-őrtanyába, rendőr-őrszobába, tehát egy központi állomásra, ahonnan a tűzriadót elrendelik. A kis településeken nem voltak villamos berendezések, így általános módon jelezték a tüzet pl.: kikiáltás~~a~~, kongatás, mozsárágyúlövés, a tűz irányának jelzése a toronyban, kürtjelekkel a lakosság fellármázása, a tűzoltók riasztása. A gyárakban, üzemekben gőzsíppal, szirénával, kürttel vagy haranggal jelezték a tüzeket.

A riasztás mikéntje a kor műszaki fejlettségének megfelelően történt. Az őrök a következő eszközökkel rendelkeztek: ~~a~~ kürt, kéthangú jelző(síp), sziréna, ködharsona, tülök, kézilámpás; a toronyőrnek jelzőzászló, jelzőlámpa, látcső, és a tájékozódáshoz a település térképe. Ahogy fejlődött a műszaki „világ", úgy a személyes megfigyelést segítették a technikai vívmányok. A távíró megjelenésével és elterjedésével könnyen és gyorsan jelezhették a tüzet az akkori tűzoltóságok felé. A távírók előtt a tűzoltókat vagy gyalogos, vagy pedig lovas futár értesítette. Először a távírót, majd később a telefonokat alkalmazták tűzjelzésre.

Az emberi érzékelés többféle módon történik. A látható füstöt és a fellobbanó lángokat a szemünkkel érzékeljük; ha még nem látjuk a füstöt, akkor az orrunkkal érezzük meg a szagát és bizonyos gázokat is; illetve a hőt a bőrünkkel érzékeljük. Előnye, hogy gyors, megbízható és érzékeny észlelési mód. Vannak hátrányai is pl.: a fenntartási költség.

Abban az esetben, ha az ember tüzet észlel, akkor próbálja meg megőrizni a higgadtságát és a nyugalmát. Magát és másokat is veszélybe sodorhat az, aki elveszti a „józan eszét". A 105-ös hívószámon azonnal értesíteni kell a tűzoltóságot, hiszen minden perc számít. A tűz vagy káreset jelzésére bármely szervezet vagy állampolgár távbeszélő készüléke igénybe

[1] Dr. Hadnagy Imre József: A tűzjelzés, fejlődése a XX: század közepéig

vehető díjtalanul. A tűzjelző személy igényelheti bárkitől, hogy a járművén a legközelebbi távbeszélő készülékhez, tűzoltósághoz, rendőrséghez, polgármesteri hivatalhoz szállítsa, vagy a jelzést helyette az illetékes szervezethez továbbítsa. Ha nincs távbeszélő a közelben, akkor bármilyen más, arra alkalmas figyelemfelkeltő módon fel kell hívni az emberek figyelmét a veszélyre. Ez történhet kiabálással, vészcsengővel, kürttel, haranggal, szirénával úgy, mint ahogy az elődeink tették a technika fejletlensége következtében.

Fontos a tűz gyors jelzése lakóház esetében, ugyanis a tűz ilyen épületben több ember életét és otthonát is veszélyeztetheti. Az ilyen lakóházakban több ember is rendelkezésre áll ahhoz, hogy a tűz jelzésével egyidejűleg az oltást is megkezdhető legyen. Ha közös használatú helyiségben következett be a tűz, a legelső teendő a füst eltávolítása a lépcsőházból. A füst elvezetésére használnak az úgynevezett füstelvezető ablakok, melyeket a lépcsőházból, földszintről és a legfelső emeletszintről lehet kinyitni. A tűzoltók kiérkezéséig tűzoltó készülékkel, vagy oltóanyaggal meg kell próbálni a lángok eloltását. A kiérkező tűzoltókat tájékoztassuk a tűz helyéről, terjedési irányáról, a bent lévő emberekről, állatokról, tárgyakról, a közművezetékek elzárási lehetőségéről, valamint arról, hogy mit tettek eddig.

Kötelező bejelenteni a tűzoltóságnak azokat a tüzeket is, amelyek emberi beavatkozás nélkül megszűntek, vagy a tűzoltóság közreműködése nélkül el lettek oltva.

Tűzjelzéskor a következőket kell közölni:

- a tűzeset, káreset pontos helye, címe (helyiségnév, kerület, utca, házszám, emelet)
- mi ég
- milyen káreset történt
- mi van veszélyeztetve,
- emberélet van-e veszélyben,
- a jelző személy neve, címe
- a jelzésre használt telefon kapcsolási száma, ~~a~~ ha a hívás nem nyilvános állomásról történt.

Ha a megadott postacím nem egyértelmű (mert nincs), vagy bonyolult a megközelítés, jelöljünk meg tájékozódási támpontot (műtárgy, rádióadó torony, gyárkémény...) illetve éjszaka, rossz látási viszonyok között, menjünk ki, vagy küldjünk valakit a tűzoltóautók elé a (fő)útra, és sötétben elemlámpával jelezzünk nekik.

Téves jelzésről akkor beszélünk, amikor valaki bejelentést tesz egy általa valóságosnak vélt káreseményről. Azonban erről nincs szó, csak a bejelentő a tartózkodási helyéről, észlelési pozíciójából a látottakat, az észlelt jeleket tűznek hiszi. Közös jellemző, hogy a szemtanú személy relatíve távolról (a szemközti házból, több száz méterről, esetenként több kilométer távolságból) , tehát nem közelről, vagy rossz látási viszonyok között (este, sötétben) látja, amit lát és ezek a tényezők keltik benne azt a képzetet, hogy tűzoltói beavatkozásra van szükség. Az ilyen bejelentésnek büntetőjogi vagy egyéb szabálysértési szankciója nincs, hiszen a bejelentő - téves megítélés alapján ugyan - csupán állampolgári, emberi kötelességének tett eleget.[2]

Például: nagy teljesítményű légkondicionáló berendezések, fűtési rendszerek tetőn elhelyezett hőcserélő egységei télen, hideg időben intenzív pára, gőzképződést produkálnak. Egy tapasztalatlan járókelő arra gondolhat, hogy ég a tető. De mint sokan tudják, hogy a tűz füstje sötét, fekete színű, mely magasra szállva oszlik szét, míg a gőz fehér, matt színű és a szabad levegőre jutva gyorsan lehűl, a tető fölött pár méterrel eltűnik. Erre a látványra számítani lehet a középületek, közoktatási intézmények, szállodák, kórházak, rendelőintézetek esetében.

A téves jelzésnek van egy rokon kifejezése, a vaklárma, amely alatt a rosszindulatú bejelentést értjük, és ez így már semmi jót nem takar. Vaklárma minden olyan jelzés, amelyet

[2] http://www.langlovagok.hu/azs/40_teves-jelzes

viccből, unalomból, vagánységnak hitt felelőtlenségből olyan eseményt, ami valójában nem történt meg. Ilyenek például a virtuális tüzek, balestek, humorosnak vélt események (kisiklott mágnesvonat, tengeralattjáró repülővel ütközött) megtörténtét próbálják elhitetni a telefonnál ülő tűzoltóval. Amikor egy vakriasztásra kivonulnak a tűzoltók, így védtelenül maradnak az elérhető területek a gyorsaság szempontjából. Ha a területükön valódi tűz vagy valamilyen káreset történik, akkor egy messzebb lévő tűzoltóság készenléti egységeit kell riasztani.[3]

A szórakozóknak talán még nem jutott eszükbe, hogy a poénkodásuk folyamán később nem-e éppen nekik, vagy valamelyik ismerősüknek lehet nagy szüksége a tűzoltókra. Valamint az sem jut az eszükbe, hogy így elveszik másoktól a túlélés lehetőségét. A felelőtlenségükkel nagy kárt okoznak a tűzoltóságnak azért, mert ezek a vonulások nagy költséget jelentenek, illetve a hívások a segélyhívó vonalakat lefoglalják. A lakosságnak szintén kárt okoznak a vaklármák, hiszen az egységek hiányoznak egy tényleges tűz vagy veszélyhelyzet felszámolásánál.

A rosszindulatú bejelentők számíthatnak a törvény szigorára. Az 105-ös segélykérő számot hívók telefonszámai minden esetben - nyilvános, lakás, vagy mobiltelefonra, titkosított számra tekintett nélkül - megjelennek a hírközpontokban ülő tűzoltók fogadóterminálján. Az ilyen bejelentő tehát büntetőjogi vagy egyéb szabálysértési szankcióra számíthat.

A szabálysértésekről szóló 1999. évi LXIX. törvény (Sztv.) 153. §-ában meghatározott valótlan bejelentés törvényi tényállását a következőket mondja ki:

„153 § (1) Aki a hatóságnál vagy közfeladatot ellátó szervnél vészhelyzetről vagy rendzavarásról valótlan bejelentést tesz, százezer forintig terjedő pénzbírsággal sújtható.

(2) Ha a hamis bejelentés alapján a hatóság vagy a közfeladatot ellátó szerv szükségtelenül a bejelentésben megjelölt helyszínre vonult vagy egyéb intézkedésre kényszerült, az elkövető elzárással vagy százötvenezer forintig terjedő pénzbírsággal sújtható.

(3) Az (1) bekezdésben meghatározott szabálysértés miatt az eljárás a rendőrség hatáskörébe tartozik.

(4) A (2) bekezdésben meghatározott szabálysértés miatt az eljárás a bíróság hatáskörébe tartozik.”

Mivel a vészhelyzet fogalmát a veszélyhelyzettől eltérően hatályos jogszabály nem határozza meg, ezért az Sztv. 153. §-ában szabályozott valótlan bejelentés tényállását - katasztrófavédelem vonatkozásában az követi el, aki:

- valótlan, vagy téves tűzjelzést ad (telefon, kézi jelzésadó működtetése, szóbeli bejelentés), illetve
- bármely műszaki mentési tevékenységet igénylő, valós alapot, nélkülöző bejelentést tesz, továbbá
- a katasztrófavédelem készenléti egységeinek (VFCS, VFSZ) riasztására valótlan eseményről tesz bejelentést.
- a beépített tűzjelző berendezés kézi jelzésadójával nem valós eseményről ad riasztást.

Az Sztv. 153. § (1) és (2) bekezdésben meghatározott szankció mellett, ha a megtévesztő jelzés szándékos volt, akkor a tűz elleni védekezésről, műszaki mentésről és a tűzoltóságokról szóló 1996. évi XXXI. törvény 8. § (4) bekezdés b) pontjában meghatározott költségtérítésnek is helye van.

3.2. A hagyományos kézi jelzésadó

A legáltalánosabb eszköz a kézi jelzésadó, melyek piros vagy zöld színű LED-del rendelkeznek. Elhelyezés szempontjából lehet beltéri vagy kültéri. Általában piros színűek, de többféle színű kivitelben is létezik. A bemenő és a tovább menő vezetékeknek külön bekötési

[3] http://www.langlovagok.hu/azs/45_vaklarma

pontja van. Rádugható csatlakozókkal rendelkezik. Potenciálmentes NO érzékelővel vannak ellátva. Az EN54-11-es szabványnak megfelelnek. Felpattintható átlátszó fedéllel vannak szerelve, - mely lehet törőüveg vagy visszaállítható műanyag lap - így elkerülhetőek a véletlenszerű működtetések és a szándékos téves jelzéseket is megnehezíti. Kulccsal visszaállíthatóak és ellenőrizhetőek. Nem szabotálhatóak, a szétszerelésre is jelzést adnak.

Normális esetben a törőüveg vagy a visszaállítható műanyag lapka felső éle tartja NO, azaz kikapcsolt állapotban a beépített mikrokapcsolót. A kapcsoló abban az esetben átvált, amikor az üveget betörik, vagy a lapkát benyomják. A LED kigyullad a jelzésadóban, a megváltozott áram a jelzőhurkon tűzjelzést okoz a központban. Ahhoz hogy a műanyag lapkát be lehessen nyomni, egy előreugró sárga sáv teszi ezt láthatóvá.

Elhelyezése:

- nem automata jelzőkészülékeket olyan helyeken alkalmazzák, ahol bármely okból nem telepíthető olyan tűzjelző készülék, amely kizárólag automata jelzőkészülékekkel használható
- üzemszerű-, vészkijáratok, kiürítési útvonalak mentén
- telepítési magassága 1,2-1,6 m között
- jól látható és megközelíthető, forgalmas helyen
- a kilincs, illetve nyitószerkezet felőli részen kell elhelyezni elkerülve ezzel a rányíló ajtószárny okozta takarást
- a terület minden pontjáról a legközelebbi kézi jelzésadót 30 m-en belül kell tudni elérni (indokolt esetben 30 méternél kisebb elérési távolság is meghatározható)

1**. ábra.** Promatt hagyományos kézi jelzésadó
Forrás: http://promatt.victorinet.hu/index.php?id=14&s=798

A jelzésadók vagy magyar felirattal vagy szimbólumos visszaállítható műanyag lappal kerülnek forgalomba. A műanyag lapok törőüvegre is cserélhetőek. A műanyag lap használata esetében a jelzésadó aktivált állapotát a műanyag működtető lapka felső szélén megjelenő sárga sáv is jelzi. A szintén megújult átlátszó, felhajtható védőfedél használatával elkerülhetők a véletlen működtetések, és megnehezíthetők a szándékos tűzjelzések.

4. TŰZJELZŐ ÉRZÉKELŐK

Ezek az eszközök jelátalakítók, melyek valamilyen tűzjellemző hatására átvitelre és további feldolgozásra alkalmas jelet adnak. A jel többféle lehet: mechanikus elmozdulás; belső nyomásváltozás; elektromos áramköri változás. Az érzékelők legfontosabb tulajdonságai, hogy az adott tűzjellemzőre megfelelő érzékenység, más behatásokra érzéketlen legyen és a megbízhatóság. Az ideális érzékelő a tüzet a kezdeti szakaszban, gyorsan és biztosan jelzi, a téves jelzések számának minimálisnak kell lennie és jó detektor

üzembiztos. Egy bizonytalan rendszer jelzései is nagy károkat képesek okozni. Hitetlenné teszi a jelzéseket, amelyeket az érintettek valódi vészhelyzetben sem fognak komolyan venni.

Téves jelzések okai:

- környezeti zavarok: adott tűzjellemzőhöz hasonló hatások
  - *a)* füstérzékelőknél: por, technológiai füst, gőz, kipufogó gázok, nagy légsebesség,
  - *b)* hőérzékelőknél: magas vagy gyorsan emelkedő hőmérséklet,
  - *c)* lángérzékelőknél: nyílt láng, hegesztés, sütés stb.
- véletlen eszköz tönkremenetel: mechanikai hibák, elektromos hibák, közvetlen behatás, korrózió hatására.
- nem megfelelően végzett emberi tevékenység: nem megfelelően végzett TMK munkák alatti jelzés, karbantartás alatt a távfelügyelet értesítésének hiányában bekövetkező jelzés stb.
- közeli elektromágneses zavarforrások: villámlás, telefon átjátszók, induktív nagyfogyasztók ki/bekapcsolási tranziensei stb.
- az eszköz belső meghibásodása: elektromos hiba, mechanikai hiba.
- jó szándékú jelzés: amikor tüzet vagy vészhelyzetet feltételezve működtetnek egy kézi jelzésadót
- rossz szándékú jelzés: amikor szándékosan, félrevezetési szándékkal működtetnek kézi jelzésadót vagy jeleztetnek be egy érzékelőt.

A téves jelzések legnagyobb része a rendszer normális üzeme alatt fordul elő. Legkorábban a felelős személy értesül róluk. Téves jelzéskor a felelős személynek fel kell jegyeznie, mikor, melyik érzékelő és miért jelzett, vagy ha nem derül ki egyértelműen, hogy mi okozta a jelzést, akkor a jelzés idején fennálló körülményeket is dokumentálnia kell. A tűzjelzőkben a téves jelzések száma több tényezőtől is függ. Egy normál irodai környezetben telepített tűzjelző esetén 1 téves jelzés 100 érzékelőnként évente még elfogadható, míg ipari környezetben 1/75 vagy 1/50 arány a gyakoribb.

Íme néhány tényező, melyek eredménye téves tűzjelzés:

- a rendszerben használt automatikus érzékelők száma (főleg füst),
- az érzékelők környezete,
- az épületben folytatott technológia, tevékenység,
- az épületben külső szervezetek által végzett munkák felügyelete,
- az elektromágneses zavarok jelenléte és nagysága,
- a rossz szándékú téves jelzések valószínűsége.

Az érzékelő gyártók törekvéseinek ellenére az egyes tűzérzékelők működési elvükből következően bizonyos környezeti hatásokra ugyanolyan érzékenyek lehetnek, mint az észlelni kívánt tűzjellemzőre. A tűzjelző rendszer tervezője általában ezeknek a tulajdonságoknak az ismeretében választja meg egy adott terület védelmére az érzékelőket. A téves jelzések az esetek többségében az üzemeltetési körülmények módosításával, a technológia előírások betartásával vagy megfelelő módosításával elkerülhetőek.

Általánosságban a tűzérzékelőknél téves jelzés generálódik, ha:

- elektromágneses vagy rádiófrekvenciás interferencia van jelen, melynek kiváltó oka a rossz kábelezés vagy az utólag telepített zavarforrások. Megoldást jelent az árnyékolt kábelek használata illetve a védőtávolságok betartása a vezetékek között.
- magas páratartalom, páralecsapódás, jegesedés, vízbehatolás, mely abból következik, hogy rosszul van szigetelve az épület tetőzete, a hűtőház valamint a kültérre szerelt érzékelő. Megoldás lehet a tömített, felületvédett elektronika vagy a fűtött páramentesített érzékelők.

- eszköz hiba, tönkremenetel bárhol és bármikor megtörténhet. Nem létezik megoldás.
- rossz szándékú jelzések nyilvánosan látogatható helyeken kézi jelzésadóknál vagy kollégiumokban, iskolákban érzékelők esetében. Megoldás az eszköz elhelyezése minél védettebb módon (pl.: a kézi jelzésadóknál átlátszó védőfedél).

Az esetek többségében nem igényelnek karbantartói beavatkozást a téves jelzések. Sokszor az épület vagy a technológia üzemeltetési körülményeinek szigorításával vagy a módosításával megszüntethetőek. Vannak olyan esetek, amikor nem módosíthatók a körülmények, ilyenkor a karbantartónak kell megoldania a problémát. A megoldás során tervmódosítás vagy tervezői jóváhagyás is igényelhető újfent.

4.1. Hőérzékelők

Ezen érzékelők csak akkor adnak jelzést, ha egy beállított hőmérsékletet érnek el. Olyan helyen alkalmazzuk őket, ahol nagy hőmérséklet-növekedés, vagy füst nélküli égés várható, illetve más típusú érzékelők nem használhatók. Nem érzékenyek a füstre, a nagy nedvességtartalomra, a szennyeződésekre. Önállóan életvédelemre telepíteni nem lehet, mérsékelt tűzkockázatú helyiségekben alkalmazhatjuk. 7,5 m-es belmagasság fölé nem helyezhető el. Az előnyük az, hogy egyszerű és olcsó szerkezetek. A hátrányuk pedig, hogy nagy a jelzési késedelem, egyrészt a tűz további szakaszához való kötődésből, másrészt a szerkezet hőtehetetlenségéből adódik, illetve abból, hogy az érzékelhető hőmennyiség valamivel később alakul ki az égés során, mint például a füst. Kizárólag beltéren alkalmazható és a tűz közelében kell lennie.

Téves jelzés a következő esetekben keletkezik ezeknél az érzékelőknél:

- túl magas helyi hőmérséklet hatására,
- helyi fűtőberendezés hatására,
- ipari folyamat hatására,
- közvetlen napsugárzás hatására.
- hirtelen hőmérsékletnövekedés télen,
- hosszabb szellőztetés után (konyhában, raktár berakodó részén).

Megoldást jelenthet:

- a magasabb jelzési hőmérsékletű típus választása,
- az érzékelő áthelyezése
- a jelzés verifikáció, mely azt jelenti, hogy egy érzékelő riasztásakor a tűzjelző központ nem fogadja el azonnal a jelzést, hanem az előre beállított idő (másodpercek) elteltével ellenőrzi újra a mért tűzjellemző szintjét. Amennyiben még mindig a riasztási tartományban van az érzékelő jelszintje, a központ elfogadja a jelzést.[4]

A hőmérsékletérzékelők jól alkalmazhatók**:**

- korrozív, poros környezetben,
- ahol nagy páratartalom, gőzképződés várható,
- karbantartási akadályok esetén,
- 60 °C-nál magasabb környezeti hőmérséklet mellett,
- konyhákban, kazánházakban.

[4] http://www.vasmagyar.hu/index.php?termekek&sub=AM1000

Nem használhatók:

- ahol kis hőmérsékletnövekedés várható,
- nagy belmagasságok esetén – önállóan életvédelemre,
- klímatizált terekben,
- gyors gőzképződésnél, illetve lánggal működő sütők esetében hősebességérzékelőt.

A hősebesség érzékelők a tényleges hőmérséklettől függetlenül, a hőmérséklet változásának bizonyos sebességénél adnak jelzést. A hőérzékelők nagy belmagasságú (h>7,5m) helységekbe nem telepíthetők, de nem érzékenyek a füstre, a nagy nedvességtartalomra, szennyeződésekre. A hősebesség érzékelők akkor jeleznek, ha a változás sebessége meghaladja a 3-5 °C/perc értéket. Minél nagyobb a hőmérséklet növekedése, annál rövidebb idő alatt jeleznek. A felügyelt terület 15-30 m^2 lehet, ezért sűrűbben kell telepíteni a hőérzékelőket.

4.2. Füstérzékelők

Ezek a leggyakrabban alkalmazott érzékelő fajták, nem kell a tüzet közvetlenül „látnia". A detektorok a füstszemcse megjelenése, mérete és optikai tulajdonságai alapján jelzik a tüzet. A tűztől származó füst szemcseméretének spektruma 0,01-10 μm-ig terjed. A szemmel látható szemcseméret tartomány 0,5 μm-től számítható. Általában pontszerű füstérzékelőkkel 30-120 m^2 védhető, a terem plafonjára szerelve. Hátrányuk az, hogy lassan érzékelnek lángoló égés során; csak beltéren alkalmazható és téves jelzést okozhatnak a zavaró környezeti hatások.

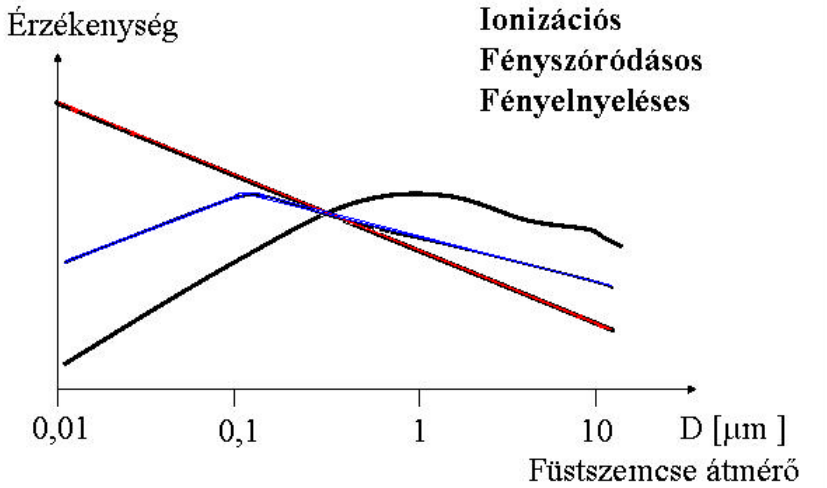
A téves jelzés leggyakoribb esetei ezeknél az érzékelőknél:

- sütéskor, főzéskor füst és gőz keletkezik a konyhában, illetve annak a környékén.
- gőzök keletkezhetnek a fürdőszoba, zuhanyzó környékén, illetve különböző ipari folyamatoknál.
- rovarok, pókok vagy muslicák kikelése, rajzása nyár vége felé, félig nyitott ipari csarnokokban.
- aeroszolok, kozmetikai füst, szállodai szobákban használt szagosítók, parfümök vagy diszkófüst.
- tömjén, gyertya, mesterséges füst templomokban, éttermekben, színházakban.
- erős légmozgás, huzat ipari csarnokok bejárathoz közeli érzékelőinél.

Ahhoz, hogy ne riasszanak be a füstérzékelők tévesen, az alábbi megoldásokkal kiküszöbölhetőek:

- az éjszakai/nappali érzékenység változtatása,
- az adaptív érzékelő,
- az együttes jelzés,
- csoport-döntés,
- kombinált érzékelő használata,
- a jelenlét (felügyelt/felügyelet nélküli) üzem alkalmazása.
- sűrű rovarvédő háló az érzékelőn a rovarok ellen
- jelzés verifikáció.

Az ionizációs füstérzékelő téves riasztást generál vágás, hegesztés, ionizáló sugárzás és villámlás esetében. Megoldást jelent az éjszakai/nappali érzékenység változtatása, adaptív érzékelő használata, jelzés verifikáció, együttes jelzés, csoport-döntés vagy kombinált érzékelő használata, jelenlét (felügyelt/felügyelet nélküli) üzem alkalmazása, illetve érzékelő vagy típuscsere.



2. ábra. A különböző elven működő füstérzékelők érzékenységének változása
Forrás: Hatvani Hivatásos Önkormányzati Tűzoltóság irattára

Vonali füstérzékelő esetében téves jelzés keletkezik:

- a sugárzás részleges vagy rövid idejű takarásakor,
- elmozdulásakor, melynek kiváltója lehet madár, villás-targonca, futó macska, instabil szerelés, épületmozgás, vagy diletáció,
- ha fals fény jut a vevőbe laposan besütő nap esetében,
- ha a vevő közelébe felszerelt nátrium-, higanygőz vagy halogén lámpa van,
- vaku villanásakor,
- rövid ideg tartó por vagy szösz pamatok vannak jelen (a huzat a szellőző rendszer, takarítás vagy a technológia a sugár útjába viszi az anyagot)
- lassú, folyamatos porlerakódás az érzékelő lencséjén vagy a reflektoron.

Megoldások a téves riasztás kiküszöbölésére:

- jelenlét (felügyelt/felügyelet nélküli) üzem alkalmazása,
- az érzékelő áthelyezése,
- a vevőbe érkező fény intenzitásának csökkentése a meglévő visszaverő felület eltávolításával vagy megszüntetésével a sugár környékéről
- az éjszakai/nappali érzékenység változtatása,
- adaptív érzékelő használata,
- jelzés verifikáció,
- a drift kompenzálást alkalmazó érzékelő, mely azt jelenti, hogy a kamra szennyeződéséből származó kamrajelnek megfelelően az érzékelő is folyamatosan emeli riasztási szintjét. Állandó értéken tartja érzékenységét az érzékelő.[5]

4.3. Láng és sugárzásérzékelők

Az égés során a tűz kibocsát a látható fénytől eltérő hullámhosszú energiacsúcsokat is. A nagyobb hullámhosszúságú IR (infravörös) és a rövidebb hullámhosszúságú UV (ultraviola, ultraibolya) tartományban is vannak energiacsúcsok. Ezeket érzékelik a lángdetektorok. Előnyük, hogy kültéren is alkalmazhatóak, a közvetlen napfényben is képesek üzemelni, gyorsan észleli a lángfázissal induló tüzeket, illetve gyors jelzésre képes nagy távolságból is. Hátrányuk az, hogy a tüzet közvetlenül „látnia" kell és elég drága eszközök.

A napsugárzásra érzéketlen, arra tévesen nem jelző érzékelőket lehet létrehozni. Ezt úgy lehet elérni, hogy a lángérzékelőknek olyan hullámhossz tartományt kell megválasztani,

[5] http://promatt.victorinet.hu/index.php?id=192#367

amelyekben a napsugárzásnak nincs hatása (ez úgy lehetséges, ha tudjuk, hogy a földet elérő napsugárzás milyen hullámhosszakon csillapítódik).

Gyakori zavarforrások lehetnek:

- fűtőtestek, kemencék, melyek általában folyamatosan bocsátanak ki energiát, gyengén a látható fény tartományában és közepes mértékben az IR tartományban
- ívhegesztés, villámlás, melyek során egy szokásos tűzhöz képest tízezerszeres intenzitású sugárzás is létrejöhet, döntően az UV tartományban. Ívhegesztéskor a láng lobogásához hasonló gyors intenzitásváltozások még nehezebbé teszik a zavaró hatás megkülönböztetését a tűztől. A villámlás spektrumához hasonló erős UV tartalmú energiabomba érheti az érzékelőket napkitörések során is.
- a fényforrások, melyek ki/bekapcsolását leszámítva folyamatos zavaró sugárforrást jelenthetnek. Az izzószálas, a halogén és a higanygőzlámpák energia kibocsátásának nagyobb része nyilván a látható fény tartományába esik, de jelentős lehet az UV tartományban kisugárzott energiájuk is (egy valós tűzhöz kb. 10%-os)
- az ember, a meleg környezet, melyek közepes intenzitású sugárzást okozhatnak az IR tartományban. Egy emberi test vagy egy kéz által kisugárzott hő az érzékelő közvetlen közelében akkora intenzitásváltozást okozhat, mint egy vizsgálati tűz kb. 30 m távolságból, azaz nem elhanyagolható, mint potenciális zavaró tényező.
- a veszélytelen tüzek is, mint a gyufa lángolása, acetilénes hegesztés vagy az ívhegesztéskor égő gyanta. Mindezek a hatások egy valós tűz spektrumához teljesen hasonló képet mutatnak, így a lángérzékelők nem is nagyon tudnak különbséget tenni egy valós tűz és egy ilyen jellegű hatás között.

Infra lángérzékelők: Közvetlen napfény lüktetése (ventillátor, víztükör) megzavarhatja működését. Kevésbé érzékel, ha takart a tűzforrás, ha sűrű füsttel ég a tűz, és ha láng nélküli tűz ég. Az érzékelők esetében általában az ablakukra lecsapódó víz vagy a ráfagyó jég okozhat érzékenység csökkenést. Téves jelzés keletkezik mozgó falombon átsütő napfény vagy fűtőberendezés által keltett meleg levegő megszaggatva a ventilátor lapátjaival. Folyamatos IR forrás (napfény vagy fűtőberendezés) nem okoz jelzést, mert az érzékelők a sugárzás villódzását is figyelik. Ezek mind zavaró IR források. Megoldás lehet a zavarforrás árnyékolása (akár ablaküveggel) vagy áthelyezése úgy, hogy ne zavarja az érzékelő látóterét, beépített jelzés verifikációval rendelkező érzékelő kiválasztása.

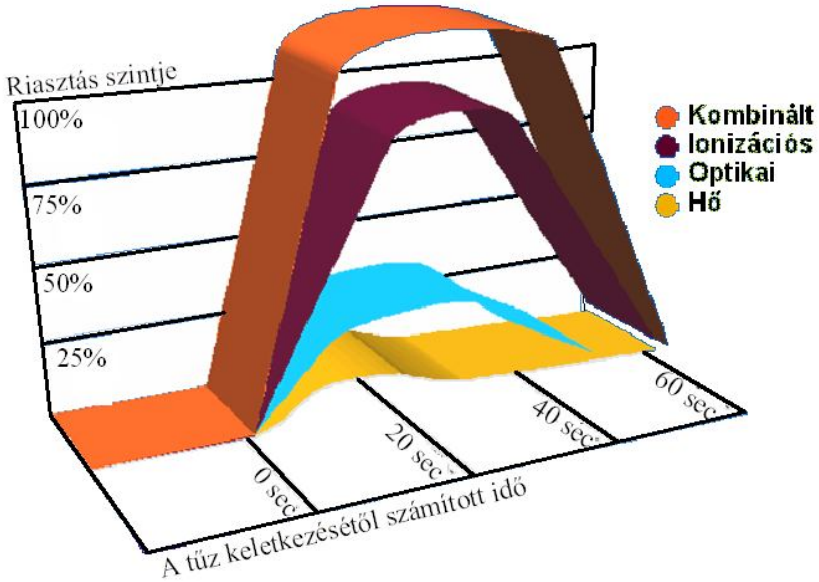
UV lángérzékelők: Érzékeny a porra, nedvességre, szikrákra, villamos ívekre és az olajszennyezésre, illetve a magas hőmérséklet is befolyásolhatja a működését. Téves jelzés keletkezik villámlás, ionizáló sugárzás (hegesztés), UV vagy kvarc-halogén lámpák esetében. Ezek mind zavaró UV források. Megoldást jelent a zavarforrás árnyékolása (ablaküveggel) vagy áthelyezése úgy, hogy ne zavarja az érzékelő látóterét, beépített jelzés verifikációval rendelkező érzékelő választása.

4.4. Kombinált érzékelők

A megnevezés alatt általában a pontszerű, kombinált hő- és füstérzékelőket értjük. Ezek az érzékelő típusok több tűzjellemzőt mérnek egyszerre, növelve a jelzés megbízhatóságát. Természetesen létezik más típusú kombinált érzékelő is (pl. gázérzékelővel kombinálva). Maguk a vonali füstérzékelők is ennek tekinthetőek, ha azok elektronikája alkalmas a levegőben a hőmérséklet miatt történő változások (remegés, vibrálás) feldolgozására. Általában érzéketlenebbek a zavaró tényezőkre. A különböző érzékelő elemek által mért jeleket úgynevezett tűzkiértékelő algoritmus dolgozza fel, mely jó hatásfokkal képes kiszűrni azokat a zavaró hatásokat, melyek csak az egyes érzékelő elemekre hatnak.

A kombinált érzékelők esetében a jelzés verifikálás bonyolultabb, mint a többi érzékelő esetében. Hosszú verifikációs idő letelte után jelez riasztást az érzékelő, ha hirtelen nagy

koncentrációjú füstöt észlel. A 30-50 másodperces verifikációs idő nem jelent gondot, mert azok a zavaró tényezők, amelyekre tévesen bejelezhetnek a füstérzékelők, általában nem járnak együtt a hőmérséklet egyidejű növekedésével. Abban az esetben, ha a hőérzékelő is növekvő jelet ad, a füstkoncentráció növekedése mellett, akkor biztos, hogy valódi tűzzel van dolga az érzékelőnek, így a verifikációs idő lerövidül, melynek következtében gyorsabban jelez.



3. ábra. Az érzékelés sebességének összehasonlítása
Forrás: Hatvani Hivatásos Önkormányzati Tűzoltóság irattára

5. TŰZJELZŐ KÖZPONTOK

A tűzjelző berendezések fejlődése mind rendszer-, mind eszköz-szinten nyomon követhető. Nem csak az érzékelésre, jeladásra használt eszközök, hanem ezek rendszerbe szervezése is sokat fejlődött az évek során.

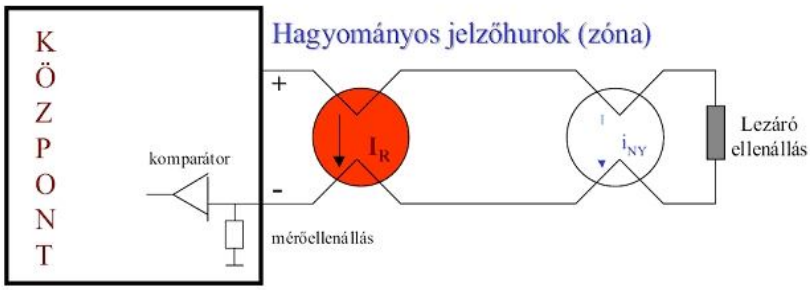
A tűzjelző rendszerek sem egyformák. A technika fejlődésével egyre szelektívebbek, pontosabbak és információdúsabbak lettek a jelzések. Az eszközök nem csupán tűz- és hibajelzés adására képesek már, hanem pontos és részletes információkat szolgáltatnak a mért fizikai jellemző értékéről, képesek tesztelni magukat, meghibásodásukról információt küldenek a központba, valamint képesek alkalmazkodni a környezeti zavarokhoz az érzékenységük automatikus vagy manuális megváltoztatásával.

A tűzjelző rendszerek életciklusát és rendeltetésszerű működését tekintve a legfontosabb tevékenység a karbantartás. A telepítés során elkövetett eseteleges hibák és tévedések a későbbiek során még orvosolhatóak, minél később, annál nehezebben és egyre nagyobb költségvonzattal (pl.: ismeretlen körülmény miatt a tervezési fázisban elkövetett hiba korrigálható a telepítés, az üzembe helyezés vagy a karbantartás során.). A legmodernebb eszközökből álló, legprecízebben telepített rendszer csak akkor lesz megbízható és stabil a működése során, ha a karbantartását rendszeresen elvégzik.

5.1. A hagyományos tűzjelző rendszer

A hagyományos rendszereknél az automatikus érzékelők és a kézi jelzésadók egy-egy hurkon sorba kapcsolva helyezkednek el. A hurok végén egy lezáró elem található, vagy egy ellenállás vagy egy kondenzátor. A központ folyamatosan figyeli az áramfelvételét az érzékelő hurkoknak. Ezeket a központokat kis rendszereknél használják. Mivel az érzékelők egy vezetékpárra vannak felfűzve párhuzamosan, így ezen az érpáron kapják a

tápfeszültséget, illetve ezen átjut vissza a jelzés a központba is. A tűz valamelyik kísérő jelenségét észlelve az érzékelők nyugalmi állapota megváltozik, és riasztási állapotba billennek. Egy komparátor áramkör segítségével mérik a hurokban folyó áramot. A központ kiértékeli az áramfelvétel változását és az értékelés eredményeképpen ad tűz- vagy hibajelzést. Azt, hogy melyik érzékelő jelzett a hurokba, nem különböztethető meg, csakis a csatornaszámot lehet beazonosítani. Amíg nem törlik a jelzést, addig a csatornára telepített érzékelőkben és jelzésadókban lévő LED-ek világítása jelzi az érzékelők aktív állapotát.



4. ábra. A hagyományos tűzjelző rendszer felépítése
Forrás: http://www.tuzjelzotervezes.hu/hagyomanyos_tuzjelzorendszer.html; (2010. 10. 10.)

Három állapot lehetséges:

- nyugalmi állapot: Nyugalmi állapotban egy meghatározott értékű nyugalmi áram folyik, aminek az értéke minimális, amit a lezáró elem állít be. Egy érzékelő hurokra 20-25 db érzékelőnél több nem telepíthető, mivel az érzékelés árammérésen alapul.
- tűzjelzés állapot: A hurkon egy riasztási áram folyik, mely a jelzést generáló érzékelőn megnövekvő áramfelvétel következménye, ami a központban jelzést vált ki. A jelzés során csak arról van információnk, hogy melyik hurokról történt a jelzés, arról nincs, hogy hol van a tűz, tehát a rendszer hurokszelektív.
- zárlat vagy szakadás: Hibaként jelzi a központ a zárlatot és a szakadást is. Ha eltávolítanak egy érzékelőt, azt a rendszer hibaként érzékeli, de a hurokban lévő többi érzékelő nem esik ki a védelemből. Az aljzatban egy dióda van elhelyezve, amely záróirányba van előfeszítve normál esetben, ha eltávolítják az érzékelőt az aljzatból, meg fog változni a diódára eső áram és nyitóirányban átengedi az áramot a hurokba.[6]

Az emberi tevékenységből származó, rövid ideig tartó zavaró hatások kiszűrésére alkalmazzák a jelzés verifikálást a hagyományos tűzjelző központokban. A lényege az, hogy az első tűzjelzést, amely beértekezett az érzékelőtől, valótlannak tekinti a központ és törli. Egy megadott ideig vár, majd megvizsgálja újra, hogy fennáll-e jelzési állapot. A verifikációs idő, azaz a várakozási idő 1-30 másodperc. Ha az érzékelő jelzésben maradt, megtörténik az igazi riasztás. Ezen módszer segítségével a nem tűztől származó, rövid ideig fennálló jelzések küszöbölhetőek ki (pl.: huzatból származó porpamacs, dízel targonca). Mivel mikroprocesszorok nem csak a központokba kerülnek beépítésre, hanem az érzékelőkben is vannak, így egy bizonyos szintű jelzés verifikálás az érzékelőkben is megtalálható.

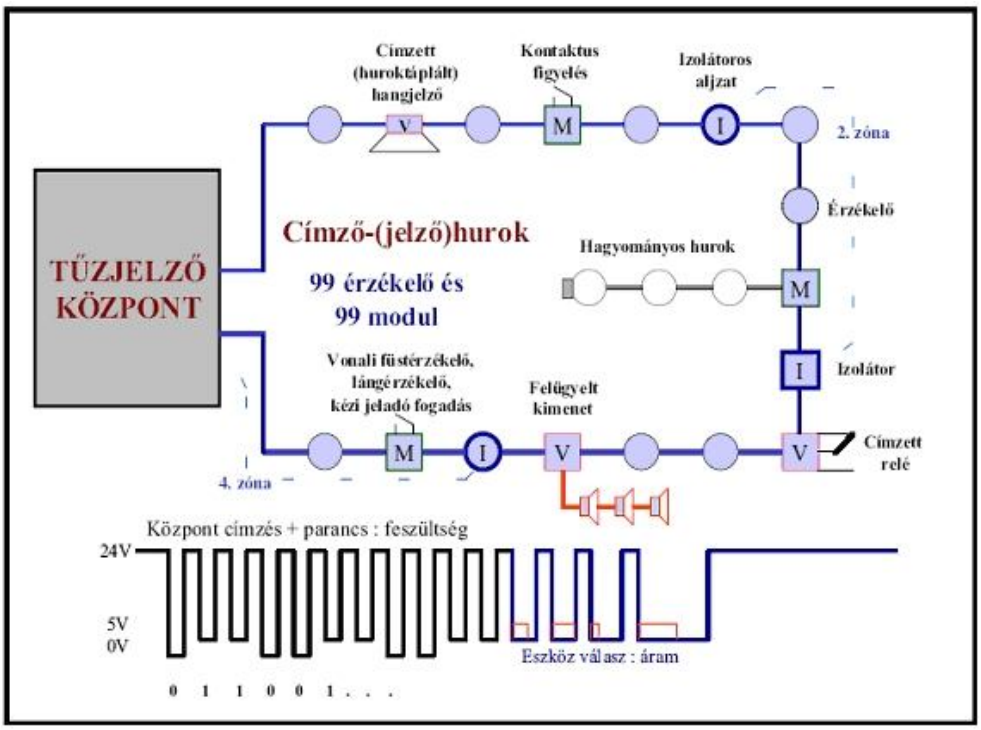
5.2. Az analóg intelligens rendszer

Az analóg szó az érzékelők működésére utal. Az érzékelők különálló műszerként vannak jelen ebben az esetben. Analóg jelet állít elő az érzékelő a mért fizikai jellemzőknek megfelelően. A központ folyamatosan kérdezi le az érzékelőket. A tűzjelző központba digitális formában érkeznek a mért értékek, a kapott értékekből kirajzolódó füstkoncentráció,

[6] http://www.tuzjelzotervezes.hu/hagyomanyos_tuzjelzorendszer.html

illetve a hőmérsékletváltozás karakterisztikáit összehasonlítja a memóriájában tárolt karakterisztikákkal. Az információk kiértékelődnek egy program szerint, amelyet telepítésekor az épület, vagy a helység tulajdonságainak megfelelően állítottak be. A központ egy speciális számítógép, hisz biztonsági termék, így a működésének megbízhatóbbnak kell lennie, mint egy személyi számítógépnek. Az érzékelők is korszerűbbek, mint a hagyományos rendszerek esetében. Egy processzort építettek az érzékelőkbe, mivel át kell alakítania a jelet analógról digitálisra.

A rendszerek a jelzőhurkok területén is újdonságot hoztak magukkal, ugyanis a központba a hurok mindkét végét bekötik. Ez a megoldás arra volt jó, hogy így már két oldalról tud kommunikálni a központ az érzékelőkkel, és ha egyszeres hurok szakadás van, akkor nem esik ki egyetlen érzékelő sem a rendszerből. Egy másik üzembiztonságot növelő eszköz az izolátor, amelyet adott szakaszokra, vagy leágazásokra építetnek be. Abban az esetben, ha zárlat van, akkor csak a két ionizátor között lévő szakasz esik ki a védelem köréből. Újabban beépített izolátorod érzékelő aljzatokat alkalmaznak, így növelik a biztonsági szintet magasabbra.[7]



5. ábra. Analóg címezhető tűzjelző rendszer felépítése
Forrás: http://www.tuzjelzotervezes.hu/intelligens_tuzjelzok.html; (2010. 10. 10.)

Mára alapkövetelménnyé vált a címezhető érzékelők alkalmazása. A technika már odáig fejlődött, hogy nem csak számok alapján azonosíthatjuk az érzékelőt, hanem neveket is tudunk hozzájuk rendeli, hiszen általában grafikus kijelzővel vannak ellátva a központok.

A téves jelzések csökkentésének az érdekében alkalmazzák a többszintű jelzést, amelyeknél egyedileg beállítható az érzékenység. Csoportokba rendezhetőek az eszközök, és együttesen figyelhetők. Különböző időpontokban és helyiségekben más lehet a mért érték alapszintje, ennek megfelelően állítható az érzékenység, tehát változó érzékenységet állíthatunk be napszakonként. Amikor elszennyeződnek az érzékelők, akkor a központ és az érzékelők is mind el tudják végezni a driftkompenzációt, tehát így ritkábban van szükség karbantartásra. Az eszköz jelzi, hogy mikor érte el azt a szintet, amikor már ki kell tisztítani (kb.: 70-80% az eredeti jelzés szinthez mérten). Lehetőség van jelzés verifikációra, amelynek

[7] http://www.tuzjelzotervezes.hu/intelligens_kozpontok.html

az a lényege, hogy az emberi tevékenységből származó zavarokat ki tudjuk küszöbölni rövidebb időn keresztül.

5.3. Az intelligens (osztott intelligenciájú) rendszer

Egy egyszerű felhasználó számára semmiben sem különbözik az analóg intelligens rendszertől, viszont egy tervező vagy egy telepítő számára a két rendszer között nagy különbségek vannak.

Az objektumok egyre nagyobbak, így egyre több érzékelőre van szükség, a számuk meghaladhatja akár a több ezret is, ezért további fejlesztésekre volt szükség. Mivel az érzékelőkben a processzorok már benne vannak, ezért csak néhány funkciót kellett átvenni a központtól. Ha az érzékelők önmagukban is képesek lesznek döntést hozni, egy kombinált érzékelőben továbbra is több tűzjellemző együttes figyelembe vételével, akkor nem kell a központtal kommunikálni csak abban az esetben, ha valamilyen eltérés mutatkozik a normál állapothoz képest. A központ feladata csak a felügyelet és a szükséges jelzési és vezérlési feladatok ellátása lesz tűz esetén.

Az ezeknél a rendszereknél használt érzékelőkre különféle kiértékelő programokat lehet feltenni, attól függően, hogy az adott területen milyen tűz várható. Ezzel a módszerrel is lecsökken a téves jelzések száma. A kombinált érzékelők működése nem egyszerű logikai „és” vagy „vagy” kapcsolat alapján működik, hanem egy beépített mikroprocesszor által végrehajtott kiértékelő program segítségével. A már telepített érzékelőkben a kiértékelő algoritmus később megváltoztatható. Folyamatosan történik a mintavételezés és csak a kiértékelés eredményét küldi el az érzékelő a központnak.

A biztonságos jelzés érdekében a veszélyszintjelzések a már előre meghatározott programozásnak megfelelően kerülnek kijelzésre és történnek meg a vezérlések. Beállítható a központ egyszerű esetre, 0-s szint nincs veszély, az 1-es szint technikai információ, a 2-es szint a figyelmeztető jelzést, a 3-as szint a riasztást váltja ki, de multizónát is beállíthatunk, ahol is a vezérlések abban az esetben indulnak meg, amikor legalább 2 érzékelő 2-es veszély szintet jelez, ilyenkor a központ is részt vesz. A 0-ás veszély szint nem kerül kijelzésre, viszont a központ eltárolja. Felhívja a figyelmet egy karbantartás alkalmával arra, hogy az adott körülményekhez képest az érzékelők vagy elszennyeződtek és karbantartást igényelnek, vagy túl érzékenyek, és az érzékelőre egy másik algoritmust kell letölteni.

A rendszerbe helyezett érzékelők telepítéskor a jelzőhurkon keresztül kapják meg a kiadott algoritmust, amit egy flash memóriában tárolnak így tápfeszültség nélkül is megőrzik az információkat. Ha meghibásodik az érzékelő és ki kell cserélni, abban az esetben a régi érzékelő helyére tett új eszközre nem kell feltölteni semmit. A központ automatikusan elvégzi a feltöltést, ezáltal a telepítők, és karbantartók munkáját megkönnyíti.[8]

A jelzés verifikálás az intelligens tűzjelző központokban is régóta alkalmazott eljárás. A drift kompenzálást először az intelligens központoknál alkalmazták, mert itt folyamatosan rendelkezésre állt a központban az érzékelők által mért tűzjellemző értéke. Amióta a mikroprocesszorok az érzékelőkben is helyet kaptak, nincs akadálya, hogy egy intelligens érzékelő vagy akár egy hagyományos érzékelő maga ellensúlyozza a szennyeződés miatti érzékenység változást. Drift kompenzáláskor a központ vagy az érzékelő a beolvasott kamrajelekből egy hosszú idejű átlagértéket képez. Az átlagértékhez képest állítja feljebb a riasztási szintjét, tartja állandó értéken az érzékenységét. A szennyeződés kompenzálása nem tarthat örökké, ezért egy adott szint elérése után a rendszer, általában "Karbantartás vagy szerviz igény" hibajelzéssel figyelmeztet a karbantartás szükségességére.

[8] http://www.tuzjelzotervezes.hu/osztott_intelligenciaju_tuzjelzok.html

6. ÖSSZEFOGLALÁS

A műszaki terület rohamosan fejlődik, mellyel a jogi szabályozás kisebb-nagyobb sikerekkel, de lépést tud tartani. A szabályokat be kell tartani, mert a szabálysértés szankciókat von maga után. Ha egyenes vagy eshetőleges szándékkal követték el a valótlan bejelentést, akkor a rendőrségnél szabálysértési eljárást kell kezdeményezni minden esetben. Sok esetben csak ismeretlen tettes ellen nyomoz a rendőrség, és a tettesek az ismeretlenségbe burkolózva nem kerülnek elő. Megelőzhetőek lennének a gyakori téves bejelentések, ha a szankcionálás szigorúbb lenne. Pl.: a vonulás költségét kifizettetni, vagy közmunka stb. A szigorúbb szankcionálás céljának annak kell lennie, hogy a tettest elrettentse a viccelődéstől. Ha bizonyíthatóan tévedésből történt a bejelenés, akkor az okozott kár, költség függvényében szabálysértési eljárást lehet kezdeményezni. Aki tévedésből tette a bejelentést, annak a személynek is kell részesülnie szankciókban, de nem olyan mértékben, mint a viccelődők. Amennyiben a költségeket nem térítik meg, úgy elzárást kellene alkalmazni. Véleményem szerint le kellene szabályozni, hogy a mobiltelefon szolgáltatók kiadják a telefonszámhoz tartozó adatokat a hatóságok számára, mert így könnyebb lenne a tetteseket utolérni és felelősségre vonni. Véleményem szerint nagyobb hangsúlyt kellene fektetni az egyes esetekre. Mindenhol oktatni kellene a téves jelzés következményeit, hátha riasztó hatása lenne és így is csökkenhetne a téves betelefonálások száma. A lakosság köztudatába azt is be kellene vinni, hogy mielőtt jó szándékból betelefonálnak, hogy tüzet látnak, vagy füstöt, előtte bizonyosodjanak meg róla, hogy tényleg szükség van-e tűzoltói beavatkozásra, mert lehet, hogy pl.: csak a szomszéd égeti az avart.

A téves jelzések soha nem szüntethetőek meg teljesen, csak minimálisra csökkenthetőek a megfelelő tervezéssel és karbantartással, amelyben az üzemeltetőnek van a legnagyobb szerepe. Minél nagyobb egy tűzjelző rendszer, annál nagyobb a valószínűsége a téves jelzések bekövetkezésének. Az OTSZ teljes mértékben szabályozza a tűzjelző rendszer létesítésének, a résztvevők feladatait és kötelességeit is. A felesleges tűzoltósági vonulások számát, melyek a téves jelzésből erednek úgy csökkenthetjük, hogy meghatározzuk az üzemeltető feladatait, felelősségét és ezek számon kérhetőségét. Az üzemeltető kapjon megfelelő szintű oktatást, melyben szó van a téves jelzésekről (kialakulás, megelőzés).

Egy tűzjelző működését veszélyeztetik mind a személyi, mind a környezeti feltételek. A felülvizsgálatok során ezeket a feltételeket is ellenőrzik, hiszen a cél az, hogy a vészhelyzetben a rendszer megbízhatóan és azonnal működjön. Ahhoz, hogy egy rendszer hosszútávon és megbízhatóan működjön, rendszeresen kell ellenőrzéseket, felülvizsgálatokat és karbantartásokat végezni. Ha a karbantartást nem szakszerűen végzik, előfordulhatnak téves jelzések! Ezek úgy küszöbölhetőek ki, ha az ellenőrzés során a távfelügyeletre menő kapcsolatot ideiglenesen kikapcsolják. Ilyenkor a távfelügyeletet végző szervnek be kell jelenteni a felügyelet szüneteltetésének okát, az ellenőrzés megkezdését és befejezését. Az ellenőrzés végeztével vissza kell állítani az eredeti beállításokat.

A tapasztalat azt mutatja, hogy a téves jelzések több mint 50%-át a nem megfelelő emberi tevékenységek és a környezeti zavarok teszik ki. A berendezések meghibásodása 1-2%. A jó szándékú téves jelzések 25%, ilyenek pl.: ha a szemetet égeti a szomszéd. Rossz szándékú téves jelzések 15%, pl.: amikor szórakozásból benyomják, a kézi jelzésadót vagy betelefonálnak, hogy nagyon nagy tűz van (holott nincs semmiféle tűzről szó). A vakriasztásokra történő vonulás rontja az állomány motivációját, és terhet jelent a tűzoltóságok számára. De nem csak a tűzoltóságok számára jelentenek terhet ezek a jelzések, hanem a közutakon is nő a veszélyhelyzet. A vonuló egységek is szenvedhetnek balesetet és nem gyakran, de szenvednek is.

Felhasznált irodalom

[1] Tolnai László: Általános tűzvédelmi ismeretek, Florian Press Kiadó, 1998. január 31.

[2] Neil Wallington: A tűzoltóautók és a tűzoltás világenciklopédiája, Athenaum 2000 Kiadó, Budapest 2005.

[3] Szűts Jenő: A tűzjelzéssel kapcsolatos gondo(lato)k, Promatt Kft., 2006.

[4] Promatt Elektronika Kft.: Útmutató a téves jelzések elkerülésére

[5] Tűzrendészet, Magyar Tűzoltó Szövetség, Budapest 1902.

[6] Dr. Hadnagy Imre József: A tűzjelzés, fejlődése a XX: század közepéig, http://www.vedelem.hu/letoltes/historia/hist11.pdf (2010. 10. 13.)

[7] Dr. Hadnagy Imre József: A 'tűz gyulladásának eltávóztatása, a 'támadotnak sebes hírül adása, harapódzásainak meggátlása, http://www.vedelem.hu/letoltes/historia/hist30.pdf (2010. 10. 13.)

[8] Laczik Dóra: Beszámoló a Hatvani Hivatásos Önkormányzati Tűzoltóságnál töltött gyakorlatról, 2009

[9] 1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

[10] 1/2003. (I. 9.) BM rendelet a tűzoltóság tűzoltási és műszaki mentési tevékenységének szabályairól

[11] 9/2008. (II. 22.) ÖTM rendelet az Országos Tűzvédelmi Szabályzat kiadásáról

[12] Horváth Árpád tü. ezredes: Állampolgári tudnivalók tűz esetén 2002., http://www.langlovagok.hu/html/tuzor/33.shtml (letöltés: 2010. október 13.)

[13] Csepregi Csaba tűzvédelmi mérnök: Beépített tűzjelző berendezésekkel szemben támasztott követelmények, http://www.tuzinfo.hu/?oldal=tuzjelzoberendezesek (2010. 10. 12.)

[14] Hagyományos és intelligens tűzjelző rendszerek: http://www.tuzjelzotervezes.hu/ (2010. 10. 10.)

[15] http://langlovagok.hu/ (2010. október, november)

[16] Utassy Sándor: Komplex villamos rendszerek biztonságtechnikai kérdései, Budapest 2009.

[17] Dr. Lukács György: Analóg áramkörök és érzékelők előadás vázlat

[18] Hatvani Hivatásos Önkormányzati Tűzoltóság irattára

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Pető Richárd
petori@freemail.hu

GÉPJÁRMŰVEK BALLISZTIKAI VÉDELME

Absztrakt

Az élet - és vagyonvédelem egyik legfontosabb és legkritikusabb megoldandó feladata a polgári- és katonai életben a gépjárművek ballisztikai védelme. A cikk röviden elemzi az élet- és vagyonvédelemre szolgáló, ballisztikai védelemmel ellátott gépjárműveket. Célja, hogy az olvasónak alapszintű ismereteket nyújtson a gépjárművek ballisztikai védelmével kapcsolatban.

The ballistic protection of vehicles is one of the most critical security challenges to be resolved (civil and military-wise) in the area of life and asset security. The following article briefly analyzes the ballistic vehicles used in life and asset security. The aim of the article is to give the readers a basic understanding of ballistic protection for vehicles.

Kulcsszavak: *gépjármű, ballisztikai védelem, lövedékálló üveg-gumiabroncs-karosszéria ~ bulletproof car, run flat tire device, bulletproof glass, bulletproof steel*

1. A BALLISZTIKA ÉS A BALLISZTIKAI VÉDELEM

A ballisztika [1] görög eredetű szó, mely lövéstant jelent. Mozgásban lévő (hajított- dobott, kilőtt) testek mozgásának törvényszerűségével foglalkozó tudományág.

Ballisztikai védelem során, elsősorban fegyverek elleni védelemre gondolunk, de ebbe a kategóriába tartoznak még a páncélelhárító rakéták, gránátok és a bombák robbanása következtében kialakuló primer és szekunder repeszek is. [2] Tehát, ha a gépjárművek ballisztikai védelméről van szó, akkor mindezek ellen együttesen kell védekezni.

A védelem szintjét több dolog is meghatározza, mint például a közvetlen környezeti tényezők. Hiszen egy háborús területen, mint például Irak vagy Afganisztán, ahol mindennaposak a lövöldözések és a fegyverek széles palettája fordul elő, ott magasabb védelmi intézkedéseknek kell eleget tenni. A következő táblázatban különféle fegyverek felsorolása található, melyekhez egy szükséges minimum védelmi szint tartozik. [3]

	Weapon	Munition	Velocity (ft./sec)	Mass (g)/Grain (gr)
T4 Handgun/Pistol Protection ***CEN: B4 NIJ: III-A ANSI/UL: 3***	 .38 Special	RN / SC 	850	10.2g/158gr
	 9 mm	FMJ / RN / SC 	1400	8.0g/124gr
	 .357 Magnum	FMJ / CB / SC 	1395	10.2g/158gr
	 .44 Magnum	FMJ / FN / SC 	1400	15.55g/240gr
	 12 Gauge Shotgun	SC 	1575	1 1/8 oz.
T6 High-power Rifle Protection ***CEN: B6+ NIJ: III ANSI/UL: 5/8***	 7.62x33mm/.30 Carbine	FMJ / RN /SC 	1970	7.1g/110gr
	 5.56x45mm (.223)	FMJ / PB / SCP1 	3070	4.1g/63gr
	 7.62x39mm	FMJ / PB / SC 	2300	8g/123gr
	 7.62x51mm NATO (.308)	FMJ / PB / SC 	2800	9.7g/150gr
	 7.62x54mm	FMJ / PB / SC 	2800	9.7g/150gr
	 7.62x63mm (.30-06)	30.06 RN / SC 	2500	14g/220gr
T7* Armor-piercing Rifle Protection ***CEN: B7 (single-shot) NIJ: IV***	 7.62x63mm (.30-06)	FMJ / PB / **AP** 	2900	10.8g/166gr

T8* **Extra Armor-piercing Rifle Protection** ***CEN: B7 (multi-shot) NIJ: IV+***	 7.62x51mm (.308)	FMJ / PB / **AP** (HC1)		2800	9.7g/150gr

Abbreviations:

AP = Armor Piercing (Special Core)
CB = Coned Bullet
FMJ = Full Metal (Copper) Jacket
FN = Flat Nose
HC1 = Steel Hard Core Mass
PB = Pointed Bullet
RN = Round Nose
SC = Soft Core (Lead)
SCP1 = Soft Core (Lead & Steel Penetrator)

1. ábra. Ballisztikai védelmi szintek (International Armoring Corporation- besorolás szerint)
Forrás: http://translate.google.hu/translate?hl=hu&sl=en&tl=hu&u=http%3A%2F%2Fwww.texasarmoring.com%2Farmoring_levels.html&anno=2; (2011. 11. 15.)

2. PÁNCÉLOZOTT GÉPJÁRMŰVEK

A páncélozott, megerősített jármű vagy jármű utólagos megerősítése szükséges, ha az általa szállított személy(ek) vagy csomag(ok), érték(ek) élet- illetve eltulajdonítás veszélyének vannak kitéve.

2. ábra. Lincoln lövedékálló személygépjármű
Forrás: http://image.motortrend.com/f/8275598+w569+h356+ar1/112news030122linctcl.jpg; (2011.09.14.)

3. ábra. MRAP
Forrás: http://www.blackfive.net/main/2009/05/baes-new-lightweight-mrap.html; (2011.09.14.)

Járművek külső támadhatóság szempontjából három fő részre oszthatóak:

- gumiabroncs
- üvegfelületek
- karosszéria

Ahhoz, hogy a jármű megfelelő védelemmel rendelkezzen, mindhárom alappillért megfelelően meg kell erősíteni.

A pénz- és értékszállító járművekre vonatkozó szabvány az MSZ 20300-as, a biztonsági üvegek áttörés- és lövedékállósági követelményeit a DIN 52290- es szabvány B/2, C/2-es fejezete tartalmazza.

2.1 Lövedékálló gumiabroncsok (Run Flat Tire Device)[4]

A járműveket gumiabroncsuk kilövésével mozgásképtelenné lehet tenni, melynek cseréje több percet is igénybe vehet. Ez idő alatt a védendő személy vagy vagyoni érték komoly kockázatnak van kitéve a támadókkal szemben. Ennek kiküszöbölésére megalkották a lövedékálló gumiabroncsokat. A következőkben két típus kerül bemutatásra, az egyik a polgári életben terjedt el, míg a másik a katonai szférában.

2.1.1. Polgári lövedékálló gumiabroncs

A gumiabroncs oldalfalát speciális anyagokkal (mint az aramid és a szénszál) erősítették meg, így a jármű kerekének kilövése esetén, a benne megszűnő légnyomás nélkül is meg tudja tartani a jármű súlyát. Peremkialakításának köszönhetően, a forgás közben fellépő erőhatásoknak ellenállva nem fordul le a keréktárcsáról, így tovább tud haladni akár 80km/h sebességgel is megtéve további 1-200km-t.

A polgári életben minden nagytömegű járműnél hasonló gumiabroncsokat alkalmaznak, mint például a tűzoltó autók, repülőgépek esetében. A nagy veszély abban rejlik, ha egy effajta nagy tömegű, haladó jármű defektet kap, akkor a kormányzása szinte lehetetlenné válik, felborulásának lehetőségével környezetére és a járműben tartózkodók testi épségére nézve óriási kockázatot jelenthet.

4. ábra. Michelin Pax rendszerű lövedékálló gumiabroncs
Forrás: http://www.bujakigumi.hu/upload/2010_02/04/126528319060398548/michelin_pax_system.jpg; (2011. 09. 14.)

2.1.2. Katonai lövedékálló gumiabroncs

A Resilient Technologies and Wisconsin- Madison's Polymer Engineering Center egy másik úton haladva, kifejlesztett egy légnyomásmentes gumiabroncsot, amit kifejezetten a háborús területeken lévő IED (Improvised Exploding Device - Rögtönzött Robbanó Eszközök) ellen biztosít védettséget a katonai alakulatoknak. A kör alakban elhelyezett, a méhek által hatszögletű viaszsejtekhez hasonló mintázatnak köszönhetően a gépjármű az önterhén kívül fellépő egyéb erőhatásokkal is könnyedén megbirkózik. További előnye, hogy zaj- és hő csökkentő hatású.

5. ábra. Lövedékálló gumiabroncs (Hooneycomb)
Forrás: http://www.markstechnologynews.com/2008/11/honeycomb-tire-bomb-proof-bullet-proof.html; (2011.09.14.)

2.2 Lövedékálló biztonsági üveg (Bulletproof Glass)[5]

A járművek másik leggyengébb pontja az üveges felületek, melyek már kisebb törmeléktől vagy légnyomás emelkedéstől is betörhetnek. Az üveg betörése kettős veszélyt is rejthet. A rajta áthaladó lövedék a gépjármű személyzetét elsődlegesen veszélyezteti, míg a másik problémát az üveg szétrobbanásakor kialakuló hegyes és éles üvegtörmelékek – más néven másodlagos vagy szekunder repeszek - jelentik az alattuk vagy közvetlen közelükben elhelyezkedőkre. Nagy sebességgel „berobbanó" kisméretű üvegszilánkok is komoly sérült tudnak okozni, mely akár halálos is lehet.

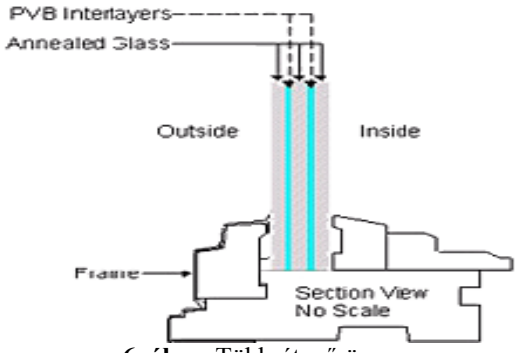
Ahhoz, hogy ezeket a veszélyforrásokat ki tudjuk küszöbölni, többféle megoldási lehetőség áll rendelkezésünkre.

2.2.1. Biztonsági fóliával ellátott törésálló üveg (Anti Shatter Film- ASF-)

Az ablak felének felületére fólia réteget visznek fel, mely az ablak (például lövedék vagy más tárgy okozta) összetörésekor összefogja azt és nem hagyja, hogy az éles repeszdarabok szétszóródjanak.

2.2.2. Többrétegű üveg (Laminated Glass)

Ennél a típusnál az ablak több réteg üvegből épül fel, anyaga PVB (Polyvinyl Butyral) gyanta, mely erőssé, átláthatóvá, hajlékonnyá és edzetté teszi azt.



6. ábra. Többrétegű üveg
Forrás: **Hiba! A hiperhivatkozás érvénytelen.**; (2011. 07. 12.)

2.2.3. Merev és hajlékony rácsrendszer (Rigid Catch Bar Systems and Flexible Catch Bar Systems)

Speciális lövedékek, mint például a robbanó lövedékek ellen fokozottabb védelmi intézkedések szükségesek. Ha a becsapódó lövedék nem is töri át az üveget, de annak becsapódásakor, az üveg közelében lévő robbanás képes egyben kirepíteni az üveget a megrongálódott ablakkeretből. Kivédésére az ablak mögé rácshálózatot építenek ki, mely már képes felfogni az üveget. További megoldást ad még a drótüveg használata vagy ezek kombinációja.

7. ábra. Lövedékálló biztonsági üveg tesztelése
Forrás: http://www.customarmoring.com/levels.html; (2011. 12. 03.)

2.3. Lövedékálló karosszéria

A harmadik támadható terület a karosszéria. Minden a karosszéria alá behatoló test a járműben (például a motorban) vagy annak személyzetében kárt, sérülést okozhat. Éppen azért, ennek a védelme akárcsak az üvegezett felületeké vagy a gumiabroncsoké nagyon fontos. Karosszéria védelmének kialakításánál 360 fokos védelemre kell törekedni, hiszen a különféle fegyverekből érkező veszély oldal és fenti irányból és érkezhet. A gépjármű alját többnyire a robbanószerkezetek és azok repeszei fenyegetik.

Lövedékek elleni védelem növelését a páncélzat erősítésével vagy új technikai anyagok, valamint ezek vegyes alkalmazásával lehet elérni. Ha a páncélzat vastagságának növelése mellett döntünk, akkor számolnunk kell az egyéb tényezők megváltozásával, mint például a jármű tömegének növekedésével. Minél vastagabb a páncélzat, annál nehezebb a jármű, minél nehezebb a jármű, annál erősebb motor szükséges hozzá, ami esetlegesen jóval több üzemanyag költséggel járhat és mindemellett az alkatrészek teherbíró képességét is növelni, méretezni kell.

Tehát ez az út nehezen járható, de akkor milyen újfajta technikai anyagokra van - lesz lehetőség?

Ilyen például a Carbon, az Aramid, a Twaron, a Spectra, a Certran, a PBO, a Dyneema és a különbféle üvegszálak alkalmazása. Nem csupán nagy teherbíró képességük miatt előnyös használatuk, hanem tömegük is jóval kisebb, megkönnyítve így a viselést és a teherhordást.

8. ábra. Lövedékálló páncéllemez
Forrás: http://www.customarmoring.com/levels.html; (2011. 12. 03.)

Jövőbeni lehetőség még a pókfonálban rejlik, aminek az átmérője az emberi hajszálnak mintegy tizede, ugyanakkor kétszer erősebb, mint az aramid szál és vagy tízszer, mint az acél.

Ezek mellett fontos tulajdonsága, hogy nem környezetszennyező és képes a lebomlásra.

A karosszéria védelmének továbbnövelésére különféle védőbevonatok alkalmasak, mint például a LINE-X[6]. Ez egy kétkomponensű, folyékony elasztometrikus poliuretán, mely gyors száradást követően csúszásmentes, vízzáró, vízálló és robbanásálló bevonatot képez.

9. ábra. Line-X –el felületkezelt gépjármű
Forrás: http://picasaweb.google.com/MillenniumLinex/MillenniumLineXXtraColor; (2011. 08. 20.)

Épületekhez, járművekhez (légi, földi, vízi: hadi- tengeralattjárók… és polgári áruszállító és tömegszállító hajók), védőöltözékekhez egyaránt alkalmas. Az amerikai katonák által használt szállítójárművek, mint például a HMMWV (High-Mobility Multipurpose Wheeled Vehicle), azaz ismertebb nevén Humvee-k vagy harci helikopterek is ilyen anyaggal felületkezeltek.

3. ÖSSZEGZÉS

A kor egyik legnagyobb kihívása a személy és vagyon védelme, kiemelten védelmük a szállítás során. Ilyenkor ugyanis nagymértékben megnő egy esetleges támadás vagy rablás kockázati tényezője.

A kockázati tényező csökkenthető aktív és passzív védelmi eszközzel, valamint az úgynevezett elrettentő hatású intézkedésekkel. Védelem kiépítés során törekedni kell a rendszerek vegyes alkalmazására, az egyik- vagy másik kizárólagos használata nem biztosít olyan hatásfokú védelmet, mintha több rendszert alkalmaznánk egyszerre. Rendkívül fontos, hogy meg tudjuk állapítani a veszélyforrások típusát azok kockázati tényezőjét. Ehhez

folyamatosan frissülő, megújuló mély és széleskörű ismeretekre van szükség, ahol az újonnan megjelenő technikai vívmányokat esetlegesen eltérő vagy létrejövő szakterületekkel ötvözve kidolgozhatjuk a védelmi koncepciókat, intézkedéseket, ellenlépéseket, legyen az polgári vagy katonai irányultságú tevékenység.

Felhasznált irodalom

[1] Ballisztika fogalma - wikipédia: http://meszotar.hu/keres/ballisztika; (2011. 11. 20.)

[2] 253/2004.(VIII.31.) Kormányrendelet: a fegyverekről és lőszerekről – törvényi meghatározás alapján; (2011.11.19.)

[3] Lövedék elleni védőszint - (Ballistic Protection Level): http://translate.google.hu/translate?hl=hu&sl=en&tl=hu&u=http%3A%2F%2Fwww.texasarmoring.com%2Farmoring_levels.html&anno=2; (2011. 11. 15.)

[4] Lövedékálló gumiabroncsok http://www.markstechnologynews.comm; (2011. 11. 10.)

[5] Pető Richárd: Terrorista robbantások elleni védekezés eszközei és lehetőségei tömegtartózkodású objektumokban, (2012)

[6] LINE-X védőbevonat: http://www.line-x.hu; (2011. 11. 27.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Rudolf Ádám
rudolf.adam88@freemail.hu

GPS RENDSZER MŰKÖDÉSE ÉS ALKALMAZÁSA A BIZTONSÁGTECHNIKÁBAN

Absztrakt

A mérnökök az évek során különböző területeken próbálták alkalmazni a GPS rendszereket. A mai napig használatos a közlekedésben, földméréseknél, környezeti kutatásoknál, hajók tájékozódásánál, előszeretettel használják a természetjárók, és ami nekünk, mint biztonságtechnikai szakembereknek fontos a biztonság érdekében való használata. Ez alatt elsősorban a műholdas gépjárművédelmet és a műholdas gépjárműkövetést értem. Ennek a két alkalmazásnak a működési elve azonos, azonban más-más célt szolgálnak. A gépjárművédelem a jogtalan cselekményekről, az eltulajdonításról adnak jelzést és segítenek az utólagos megtalálásban, míg a műholdas gépjárműkövetés esetében minden információ tárolódik és bármikor hozzáférhető lesz. Az utóbbi alkalmazás esetében online kapcsolat alakul ki a távfelügyelet és a gépjármű között.

Engineers tried to apply the GPS in several different areas. Nowadays this technology is used in traffic, land surveying, environment researches and the orientation of ships. The technology is also used by hikers. What's more important for us, security expert is the use of GPS for security purposes. It primarily includes the protection of vehicles via satellites and the tracking of vehicles via satellites. The principle of operation in both cases is the same but the purposes are different. In case of vehicle protection, the GPS signals illegal activities concerning the vehicles and helps with finding the vehicles later. However, in case of vehicle tracking all the information is stored and becomes available at any time, In the latter case there is continuous online connection between the base of operation and the vehicle.

Kulcsszavak: *GPS, műholdas gépjárművédelem, műholdas gépjárműkövetés ~ GPS, protection of vehicles via satellites, tracking of vehicles via satellites*

1. A GPS KIALAKULÁSA, TŐRTÉNETE

A GPS szó hallatán manapság már szinte mindenkinek a gépkocsik szélvédőjén lévő navigációs berendezés jut az eszébe. De nézzük meg mi is az a GPS és tekintsük át fejlődésének történetét.

A GPS (Global Positioning System, azaz Globális Helymeghatározó Rendszer) egy olyan műholdakból álló hálózat, amelyek a bolygó körül keringenek és jeleket sugároznak, melyeket a GPS vevők képesek fogadni.

A jelek időkódokat és földrajzi adatokat is tartalmaznak, így a felhasználó képes a pontos helyzetét, sebességét és az időt is meghatározni.

A GPS-t, számos más technikai megoldáshoz hasonlóan, először katonai felhasználásra fejlesztették ki, majd egyre nagyobb tért hódított a polgári élet széles területén is.

A globális helymeghatározó rendszert katonai és felderítési céllal az 1960-as években kezdték kifejleszteni, de az ötlet már 1957-ben a szovjet Szputnyik1 mesterséges hold fellövésekor megszületett. A tesztelések során ugyanis a mérnökök arra lettek figyelmesek, hogy a műhold által kibocsátott rádiójelek hullámhosszainak változásait elemezve pontosan meg tudták határozni a műhold helyzetét.

Az Egyesült Államok 1960-ban alkotta meg a Transit nevezetű műholdas rendszerét, mely a tengeralattjárók és a felszíni hajók helymeghatározását segítette. Ez a rendszer összesen 5 db műholdból állt, amely lehetővé tette, hogy egy hajó óránként egyszer meghatározza helyzetét a tengeren.

1967-ben megjelent a Transit utódja, a Timation műhold, majd a katonai célú GPS-ek gyors fejlődésnek indultak.

A következő fontos évszám 1978, amikor is polgári célokra is felhasználhatóvá tették a GPS-t, hogy a légiközlekedés, a hajózás és a szárazföldi közlekedésben résztvevő járművek helyzete pontosan meghatározható legyen, ezzel segítve a veszélyes területek elkerülését.

A kezdeti helymeghatározó rendszereknek több hátrányai is voltak. A viszonylag kisszámú műholdak szűk észlelési ablakot biztosítottak (15-20 perc/átvonulás), így sokat kellett várni a következő mérésre. Egy-egy mérés pontossága 50 méter volt, így több mérés átlagát kellett venni a pontosabb helymeghatározáshoz. Ebből következik, hogy a gyorsan mozgó tárgyak pontos navigációjára nem voltak alkalmasak. Továbbá a műholdaknak igen alacsony volt a pályamagasságuk így azok nem voltak stabilak.

Egy újfajta fejlesztési irány vált tehát szükségessé, melynek követelménye az volt, hogy az időjárástól függetlenül, a nap 24 órájában, akár mozgó tárgyak esetében is, gyors és pontos helymeghatározást biztosítson.

Az Egyesült Államok és az akkori Szovjetunió versenybe szállt egymással. Előbbi a NAVSTAR GPS, míg utóbbi a GLONASS nevű rendszert fejlesztette ki.

Amerika 1973. december 17-én mutatta be 24 műholdból álló rendszerét és a teljes kiépítettségét 1993 nyarára érte el. Ma ezt a 24 műholdból álló rendszert nevezzük globális helymeghatározó rendszernek (GPS). A 24 műhold közül 21 db mindig aktív és 3 db tartalékként szolgál.

A Szovjetunió bukása miatt a GLONASS soha nem érte el a teljes kiépítettségi szintjét. [1] [2]

2. A GLOBÁLIS HELYMEGHATÁROZÁS MŰKÖDÉSI ELVE

A GPS egy olyan helymeghatározó rendszer, amellyel 3 dimenziós helyzetmeghatározást, időmérést és sebességmérést végezhetünk földön, vízen vagy levegőben. A GPS rendszer lényege a műholdas távolságmérés.

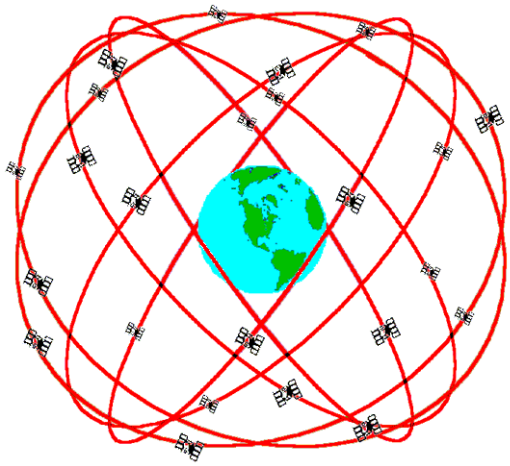
Mivel ismerjük a rádióhullámok terjedési sebességét, két nagyon pontos órával (atomóra), és a rádióhullám kibocsátásának és beérkezésének idejének ismeretével, meghatározhatjuk a forrás távolságát.

A rendszer felépítése:

- 24 db műhold
- 5 db földi monitor állomás
- GPS vevőberendezés

A GPS rendszer tehát 24 db műholdból áll, melyek közül 21 db aktív és 3 db tartalék. Ezek a műholdak 20200 km magasságban, 12 óránként kerülik meg a földet. 6 orbitális síkban (síkonként 4-4 egység) helyezkednek el és a pályasíkon egymáshoz képest 60 fokkal el vannak forgatva, míg az egyenlítőhöz viszonyított pályaelhajlásuk 55 fok.

Az 1. ábrán a 24 db műhold pályája látható a föld körül.



1. ábra. A 24 db műhold pályája
Forrás: http://astro.u-szeged.hu/szakdolg/vegiandras/felhasznalas/helymeghatarozas.html; (2011. 10. 19.)

A műholdak szabályos időközönként kibocsájtott jelei tartalmazzák a műholdak pontos helyzetét és a rajta mérhető pontos időt. Az időt nagy pontossággal kell küldeniük, hiszen ez a rendszer alapja. Ezt úgy oldották meg, hogy minden műholdba található 2 db cézium vagy rubidium atomóra. A műholdak szinkronizáltan működnek, tehát óráik össze vannak hangolva és a jeleket is egy időben küldik a megfigyelő felé.

A rendszer pontos működésének másik feltétele a műholdak helyzetének pontos ismerete.

Hogyan tudjuk meghatározni a 20200 km magasságban lévő műhold helyzetét mm-es pontossággal? A titok a nagy távolságban rejlik. Mivel a műhold jóval a földi atmoszféra felett kering, pályája nagy pontossággal kiszámítható. Sok GPS vevő memóriája tartalmazza az ún. almanach-ot, ami a műholdak pillanatnyi helyzetét tartalmazza.

Bár a nagy keringési magasság miatt a földi atmoszféra már nem befolyásolja a műholdak pályáját, az USA védelmi minisztériuma (a DoD - Departement of Defence) a precízebb helyzet-meghatározás érdekében létrehozta a földi figyelő és követő hálózatát. Ennek a hálózatnak a feladata a GPS műholdak követése, napi vizsgálata, az aktuális pozícióik és sebességük mérése, az esetleges pálya- és egyéb korrekciók végrehajtása és ezen pontosított adatoknak az elküldése a műhold felé.

A GPS műholdak 2 frekvencián sugároznak. Ezt a két frekvenciát L1-nek (1575,42 MHz) illetve L2-nek (1227,60 MHz) nevezik. A két különböző frekvenciára azért volt szükség, mert míg az L1 a navigációs adatokat és az SPS (Standard Positioning Service) kód jelet küldi, addig az L2 az ionoszférikus és más zavaró tényezőkből adódó módosítás adatait és a PPS (Precise Positioning Service) kód jelet küldi.

SPS jellemzői:

- A civil életben használatos
- 100 méter vízszintes irányú pontosság
- 156 méter függőleges irányú pontosság
- 340 nanosecundum időbeni pontosság

PPS jellemzői:

- Pontosabb mérés érhető el vele, mint az SPS-el
- 22 méter vízszintes irányú pontosság
- 27,7 méter függőleges irányú pontosság
- 200 nanosecundum időbeni pontosság

Miután 1988-ban polgári felhasználásra is engedélyezték a GPS rendszer alkalmazását, tartva attól, hogy ellenséges szervezetek is felhasználhatják, a műholdak kétféle kódot sugároznak. Az egyik az ún. C/A (coarse/acquisition), amelyet polgári használatra szántak és 15 méteres pontosságot biztosít, a másik pedig az ún. P(Y) kód (Precision code), melynek pontossága 1 cm és kizárólag titkos katonai GPS-vevővel lehet dekódolni, szabadon nem hozzáférhető.

1994 és 1998 között az Egyesült Államok a polgári felhasználású kódot mesterségesen még tovább rontotta. Ezt az ún. SA (selective availability) zavaró jel sugárzásával oldották meg. A GPS civil vevők pontossága így 150-300 méter fölé csökkent.

Nemzetközi nyomásra végül Clinton elnök, 2000. május 2-án hajnalban, megszüntette a zavaró jelek sugárzását. Így a valós idejű helymeghatározás pontossága megnőtt és a gyakorlatban néhány méteres pontosság is elérhetővé vált.

A földi monitor állomások (2. ábra) feladata, hogy nyomonkövessék, és pontos adatokat szolgáltassanak a műholdak pontos helyzetéről. Világszerte 1 db fő- és 4db segédállomás található.

2. ábra. Földi monitor állomások;
Forrás: www.soltvadkert.hu/media/konferencia_2007/a_gps-rendszer.ppt; (2011. 10. 23.)

A rendszer utolsó építőköve a GPS vevőberendezés. Ez a kézzel fogható, mindenki számára ismert felhasználói vevőegység. Ez a vevőberendezés szintén tartalmaz egy nagy pontosságú kvarcórát. A rádiójelek a műholdból némi késéssel érkeznek a vevőkészülékbe. 20200 km magasságban a késés 0,06 másodperc. A vevőkészülék figyeli, hogy a jelek különböző műholdakról milyen időkéséssel érkeznek egymáshoz képest. A késésből a vevőkészülék kiszámolja a műhold tőle mért távolságát.

Kétdimenziós rendszerben (síkon belüli) helymeghatározáshoz elegendő 3 db különböző műholdról érkező jel egyidejű vétele, háromdimenziós helyzetazonosításhoz (ha pl. a tengerszint feletti magasságra is szükség van), akkor már legalább négy műhold jeleinek a vétele szükséges. [1] [3] [4]

3. A GPS ALKALMAZÁSA

A GPS rendszerek, a polgári életben történő elterjedése révén, igen széles körben alkalmazhatóak lettek. Nézzünk ezek közül néhányat:

- Közlekedési (civil, teherszállítás, rendőrség, tűzoltóság, mentők, autóbuszok)
- Gépjárművédelem (lopás ellen)
- Geodézia, földmérés
- Természetjárás
- Környezeti kutatás (madármegfigyelés, vonuláskövetés)
- Játékok

Láthatjuk, hogy minden olyan területen hasznos eszközzé vált, ahol helyzet-meghatározásra van szükség. Számunkra, mint biztonságtechnikai szakembereknek a biztonság és az ebből következő helyzetmeghatározásban nyújt segítséget.

A GPS rendszerek műszaki megoldásai és alkalmazhatóságuk e területen napról napra fejlődik. A gépjárművekbe beépített GPS rendszerek kezdetben az utólagos megtalálást szolgálták, azonban mára már a valós idejű nyomkövetés és a különböző, leggyakrabban a fuvarozókat érő, lopások kiszűrésére is alkalmasak lettek.

A GPS alapú helymeghatározó rendszerek gépjárművekben történő megjelenése a ’90-es évek végére tehető, amikor mind a fejlesztők, mind a felhasználók rájöttek, hogy a hagyományosnak mondható mechanikai gépjárművédelmi eszközök (kormányzárak, váltózárak és immobilizerek) és a hagyományos riasztó rendszerek (villogó és hangjelző szerkezetek) már nem jelentettek komoly akadályt a tolvajoknak. [5]

Az utólagos megtalálást elősegítő berendezések, mint a GPS rendszerek, a jármű ellopását nem akadályozó rendszerek, de a járműbe beépített eszköz(ök) segítségével lehetővé teszik annak azonosítását, felkutatását és helyzetének pontos meghatározását.

Ma, Magyarországon már egyre több gépjárműben van műholdas védelem, de ez leggyakrabban csak a felső, kisebb számban a felső-középkategóriás gépjárművekre jellemző. Az ok egyszerű. A tulajdonosok e rendszerek magas költségével magyarázzák alkalmazásuknak hiányát. Ilyen rendszert már pár tízezer forintért be lehet építtetni a járművünkbe és a havi költsége sem haladja meg a pár ezer forintos tételt. Mérlegelni kell! A mérleg egyik oldalára tegyük a rendszer költségét, a másikra az ellopott autó értékét és a vele járó bosszúságokat. Máris világossá válik, hogy a mérleg melyik irányba mozdul el. Sajnos a legtöbb autós, úgy véli, hogy ez vele úgy sem történik meg, aztán egyszer csak ott állnak a parkolóban és hűlt helye az autónak. [5]

A GPS védelmi rendszer önmagában, távfelügyelet hiányában nem eredményes. A gépjárműbe telepített szerkezet tartalmaz egy sim kártyát, amelyen keresztül 24 órás online GPRS kapcsolat jön létre a diszpécserszolgálattal. Amennyiben riasztás történik, a központban a rendszer szoftver azonnal jelez, láthatóvá válik a jármű helyzete és útvonala (haladásának iránya és sebessége), majd a tulajdonossal való egyeztetés (téves intézkedés elkerülése végett) azonnal megkezdik az intézkedést az illetékes szervek bevonásával belső szakmai protokoll szerint.

A piacon találhatunk olcsó GPS gépjárművédelmi rendszereket is, melyek egy sms-t küldenek a telefonunkra a riasztás megtörténtéről. Ne elégedjünk meg ezzel! [6]

A GPS gépjárművédelmi rendszer továbbfejlesztéseként kialakultak és napjainkban egyre inkább elterjedőben vannak a gépjárműkövető rendszerek, melyek már magukba foglalják az utólagos megtalálást segítő GPS gépjárművédelmi rendszerek előnyeit is.

4. MŰHOLDAS GÉPJÁRMŰKÖVETŐ RENDSZER

A GPS gépjárműkövetés számos előnyt jelent elsősorban a gépjárműflottával – személygépkocsitól a kamionig – rendelkező cégek számára. Egy átlátható, tervezhető, és ellenőrizhető logisztikai rendszert biztosít gépjárműveik kezelésére, és ellenőrzésére. A rendszer használatával megvalósulhat a gépjárművek pillanatnyi helyzetének meghatározása, menetlevelek és kimutatások elkészítése, a gépjárművek ellenőrzése, megkülönböztethetővé válik a hivatali és magánút, optimalizálható a járművek futása vagy akár az üzemanyagszint és raktárhőmérséklet figyelése.

A rendszer úgy lett kifejlesztve, hogy interneten keresztül bármikor, bárhonnan könnyedén megvalósulhat a valós idejű lekérdezés.

A rendszer 3 szakaszból áll:

- *A járműbe elhelyezett eszköz:* A gépjárművekbe szerelt készülék egy nagy érzékenységű GPS-vevőt, valamint egy GSM egységet tartalmaz. A GPS vevő a nap 24 órájában képes meghatározni a jármű pozícióját néhány méteres pontossággal. Az így kapott adatokat a készülék a belső memóriájába rögzíti, majd egy előre beállított értéknek megfelelően bizonyos időközönként GSM csatornán keresztül továbbítja a térképes szoftver felé. A készülék optimális működéséhez szükség van GPRS és GSM lefedettségre is.
- *GSM adatátvitel a jármű és a térképes szoftver között:* A rögzített adatok GSM hálózaton keresztül, GPRS kapcsolat útján jutnak el a térképes szoftverhez. Ha a GSM lefedettség nem teszi lehetővé a GPRS kapcsolatot, akkor a belső memóriába addig fognak rögzülni az adatok, amíg a GPRS kapcsolat helyre nem áll. Ekkor fogja elküldeni a kimaradt adatokat, így egyetlen pozíció sem vész el. Az adatok tömörítve kerülnek átvitelre. A GPRS (General Packet Radio Service) adatátvitelt a szolgáltatok nem percalapon, hanem adatmennyiség alapján számlázzák, tehát az elküldött adatok mennyisége (KB) számít. Ezzel a megoldással az online felügyelet olcsóbbá vált.
- *A térképes szoftver és a tárolt adatok megjelenítése:* A gépjárművekbe telepített készülékekről az adatok a térképes szoftverbe kerülnek, ahol egy adatbázisban rögzülnek. Ezt az adatbázist különböző szintű jelszóval lehet védeni, így az adott jármű adatait csak az láthatja, akinek ahhoz jogosultsága van.

A tárolt adatokat 3 módon is megtekinthetjük:

- A WEB-en történő megtekintéshez internetkapcsolatra van szükségünk és egy PC-re. A megfelelő szintű jelszóval belépve megtekinthetők az adatok. Lekérhető egy-egy jármű pillanatnyi pozíciója, egy adott idő-intervallumhoz tartozó megtett út. A térképen egyszerre több jármű több adata is megjeleníthető.
- Kézi számítógépekre (PDA) optimalizált felületen is megtekinthetők a gépjárművek adatai. Akár mobil internet eléréssel is gyorsan és kis adatmennyiséget felhasználva lekérhetők az adatok.
- WAP böngészővel rendelkező mobiltelefonnal is lehetőség van a térképek megjelenítésére. Így akár hagyományos mobiltelefonnal is megtekinthetők a gépjárművek pontos helyzete.

Az online valós idejű GPS nyomkövetés révén tehát folyamatosan nyomon követhetők a gépjárművek és gépkocsivezetők földrajzi helyzetei és pillanatnyi elfoglaltságuk. A különböző beállításoktól függően a műhold alapú GPS flottakövető rendszer révén – a világ bármely pontjáról – ellenőrizhetők a járművezetők, látható, ha a járművezető eltér a megadott útvonaltól, kötelező megállási helyektől, vagy a szabályoktól eltérően vezet, esetleg indokolatlanul tankol. Mivel a műholdas GPS flottakövetés során ellenőrizhetők a

járművezetők, költséghatékonyabb gazdálkodás, illetve az adminisztrációs munka könnyítése valósítható meg. [7]

A költséghatékonyabb gazdálkodást lehetővé tevő alkalmazások közül nézzünk most meg kétféle megoldást.

5. ÜZEMANYAG FELHASZNÁLÁS ÉS LOPÁS RÖGZÍTÉSE, JELENTÉSE

A nagy gépjárműflottával – személygépjármű, kamion - rendelkező cégek számára az üzemanyaglopások okozta károk nagy gondot jelentenek. Régen a cégek vezetői kénytelen voltak megbízni alkalmazottaikban, hogy meg sem fordul a fejükben a céges autóból ellopni az üzemanyagot. A technikai fejlődésnek köszönhetően azonban a kellemetlenségek elkerülése érdekében a lopások ellen az okos cégtulajdonosok elkezdtek védekezni. Kezdetben a tanksapka zárásával, plombázásával védekeztek, majd jöttek azok a lopásgátlók, amelyeket a tank betöltőnyílására fixen és oldhatatlanul rögzítettek, így akadályozva meg, hogy szivattyúval vagy egyszerű lopócsővel leszívhassák az üzemanyagot.

A műholdas gépjárműkövető rendszer e területen is megoldást nyújt a probléma kezelésére. Napjaink korszerű járművei esetében a legelterjedtebb technológiát és legpontosabb adatokat az FMS vagy a CAN-bus alapú mérés jelenti. Ezekkel a megoldásokkal lehetőség nyílik a ténylegesen, a motor által elégetett üzemanyag mennyiségének mérésére, akár ±1%-os pontossággal, tehát az üzemanyaglopás megakadályozása megvalósulhat. A kiolvasott adatokat a felhasználónak GSM alapú GPRS hálózaton keresztül küldi el a rendszer. [8]

Igazából az átfolyásmérő az egyetlen eszköz az üzemanyaglopás megakadályozása esetében, amely megközelíti ugyan a CAN-bus technológia által mért adatok pontosságát, de ez a műszaki megoldás egyrészt drága, másrészt a tartály és a motor között továbbra is hagy méretlen szakasz.

Az üzemanyag figyelő rendszer alapja a gépjárműbe szerelt hardver, mely össze van kötve az FMS vagy a CAN-bus rendszerrel illetve található benne egy kommunikációs egység is, ami GPRS hálózaton küldi az információkat a megjelenítő szoftver felé. A szoftver segítségével a felhasználó igényének megfelelően diagramos vagy táblázatos formában is megjeleníthetők az üzemanyag felhasználásra vonatkozó információk illet az eltérések. Az eltérések a kiértékelés során okot akadnak az üzemanyaglopás gyanújára.

Kezdetben ezek a rendszerek nem voltak valós idejűek, tehát ezek az adatok csak akkor voltak lekérdezhetőek, amikor az adott gépjármű visszaérkezett a telephelyre. A fejlesztések révén lehetőség nyílt az online kapcsolatra, így az adatokat bármikor lekérdezhetjük, sőt beállíthatjuk, hogy automatikusan küldje a felhasználónak az üzemanyag fogyasztással kapcsolatos mérési adatokat. [8]

A járműkövetési funkció révén megvalósítható tehát az üzemanyag menedzsment, így csak a tényleges üzemanyag használat utáni költségek maradnak fent.

Megállapítható tehát, hogy a GPS alapú, műholdas nyomkövető rendszer egyszerűbbé teszi a flottakezelést, pontos üzemanyagszint mérést tesz lehetővé, és segít az üzemanyaglopás megakadályozásában.

6. HŐMÉRSÉKLETFIGYELŐ

A műholdas gépjárműkövető rendszer révén megvalósulhatnak a hűtőkocsik valamint a termékek védelmei is az online hőmérsékletfigyelő rendszer segítségével.

A rendszer rögzíti a jármű és/vagy szállítandó termékek hőmérsékleti adatait. Működési elve hasonló a fent említett üzemanyag ellenőrző rendszerhez, annyi különbséggel, hogy a

mérés telepített érzékelőkkel történik. Az érzékelők által mért értékek online módon szoftver segítségével megjeleníthetők és riasztási szint is beállítható.

Egy tipikus hűtőkocsi esetén 2 érzékelő beépítése ajánlott. Ezzel biztosítani tudjuk, hogy az ajtónál és a raktér átellenes végében mért hőmérséklet különbsége ne haladja meg a riasztási értéket.

Amennyiben a hőmérséklet hirtelen, nagymértékben megváltozik, a rendszer azonnali riasztást küld a gépkocsivezető vagy az irodában tartózkodók számára, mielőtt bármilyen kár keletkezne a szállítmányban. [9]

Ezzel a megoldással tehát a hőmérséklet jelentős csökkenéséből adódó kockázatok hatékonyan csökkenthetők.

Felhasznált irodalom

[1] Földrajzi helymeghatározás, a GPS; http://astro.u-szeged.hu/szakdolg/vegiandras/felhasznalas/helymeghatarozas.html; (2011. 10. 19.)

[2] A GPS technológiáról; http://eu.mio.com/hu_hu/global-positioning-system_a-gps-tortenete.htm; (2011. 10. 19.)

[3] A GPS rendszer; www.soltvadkert.hu/media/konferencia_2007/a_gps-rendszer.ppt; (2011. 10. 23.)

[4] Kovács Tibor - Megtalálást elősegítő eszközök, lehetőségek, Főiskolai jegyzet, 2007

[5] GPS járműkövetés; http://www.szabokriszta.hu/irasaim/gps-jarmukovetes; (2011. 10. 25.)

[6] Nyomkövetés; http://nyomkovetes.blogspot.com; (2011. 11. 03.)

[7] Műholdas gépjárműkövető rendszer; http://www.kockaforma.hu/jarmukov_b.htm; (2011. 11. 03.)

[8] Online GPS járműkövetés; http://www.webbase.hu/GPS_jarmukovetes.html; (2011. 11. 03.)

[9] Hőmérséklet figyelő; http://www.autogps.hu/features/tempmonitor.aspx; (2011. 11. 03.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Tajti Balázs
globee@freemail.hu

A BIOMETRIKUS UJJNYOMAT AZONOSÍTÁS ALKALMAZÁSÁNAK ÚJ LEHETŐSÉGEI

Absztrakt

Az emberiség létszámának gyarapodása megköveteli minden ember pontos azonosítását. Egyedül a biometrikus azonosítás alapul az emberek valódi, tőlük elválaszthatatlan azonosságán. A biometrikus azonosítás technológiája napjainkban egyre nagyobb teret hódít, és előre láthatólag ez a térhódítás csak gyarapodni fog. Rohamos elterjedése és széleskörű alkalmazhatósága miatt választottam kutatásom témájául ezt az azonosítási módszert. Kutatásom célja hogy bemutassam a személyazonosítás biometrikus lehetőségét és azok módszereit, részletesen ismertetve az ujjnyomat azonosítás technikáját. Kutatásom során elemeztem a biometriával foglalkozó cikkeket, tanulmányokat és internetes forrásokat, hogy az ujjnyomat azonosítás jövőbeli használhatóságáról és lehetőségeiről tájékozódjak, illetve hogy ezzel összefüggésben megismerjem az emberek véleményét a biometrikus formájú személyazonosítás módszerével kapcsolatban.

The growth of the population requires the accurate identification all of the people. Only biometric authentication based on people's real identity, which is inseparable from them. The biometric identification technology is becoming more and more popular, and this expansion will increase. Rapid spread and wide applicability is the reason, why I choose this identification method for my topic. My research aims, to demonstrate the possibility of biometric identification, its methods, and describe the fingerprint identification technique. During my research, I analyzed the use of biometrics from articles, studies, and internet resources, to get information about usability and possibilities about fingerprint identification, as well as get to know people's views of the form of the biometric identification method.

Kulcsszavak: *biometria, ujjnyomat, azonosítás ~ biometric, fingerprint, identification*

1. BEVEZETÉS

Az emberek pontos azonosításához évtizedek óta szerepelnek személyi igazolványunkon, gépjárművezetői engedélyünkön, útlevelünkön a legfontosabb azonosító tulajdonságaink, nevünk, címünk, születési dátumunk és helyünk. A számítógépes világban mindezen információk adatbázisokban szerepelnek, ahol mindannyian az igazolványainknak megfelelően egy-egy számsor szerint megtalálhatóak vagyunk. Bár ezen dokumentumaink rendelkeznek a pontos azonosításhoz szükséges arcképünkkel, az egyértelmű azonosításhoz mégis további egyedi azonosítókra van szükség. A biometrikus azonosítás nem más, mint bizonyos biológiai jellemzőink (ujjnyomat, kézgeometria, tenyérnyomat, írisz vagy retina vizsgálat, stb.) szerinti személyazonosítás. Ezeket a tulajdonságainkat speciális műszerekkel lemérik, majd digitális jelekké alakítva számítógépes adatbázisokban tárolják. Az azonosítás során ezen tulajdonságainkat vetik össze az adatbázisban szereplővel. A biometrikus azonosítás technológiája napjainkban egyre nagyobb teret hódít, és előre láthatólag ez a térhódítás csak gyarapodni fog.

2. BIOMETRIKUS AZONOSÍTÁS ÁLTALÁBAN

Mielőtt ismertetném a biometrikus azonosítás alkalmazását, fontosnak tartom, hogy információt adjak a szóban forgó azonosítási technikáról, ismertetve hol szerepel a személyazonosítás területén.

A személyazonosítás alapvetően az alábbi elveken alapul:

- Azonosító információ
- Azonosító tárgy
- Biometrikus azonosító

Azonosító információ: Valamilyen általunk ismert információ alapján. Általában numerikus kód vagy alfanumerikus jelsorozat (PIN, jelszó). Hátránya hogy az ember jelszavát elfelejtheti, ellophatják, vagy feltörhetik. Egyetlen előnye az egyszerűsége és olcsósága.

Azonosító tárgy: Valamilyen tárgy birtoklásán alapszik (belépőkártya, igazolvány, kulcs). Hátránya hogy könnyen elveszíthetjük, vagy ellophatják.

Biometrikus azonosítás: Ahogy bevezetőmben is említettem, a biometria nem más, mint a személyazonosítás egy olyan fajtája, ahol az ember egyedi biológiai jegyein, élettani vagy viselkedési jellemzőin alapul az azonosítási eljárás.

Az egyértelmű azonosításhoz az alábbi egyedi, személyenként eltérő jellemzőket használják:

Ujjnyomat-	Írás-
Tenyér és csuklónyomat-	Írisz-
Talplenyomat-	Retina-
Kézgeometria-	Hang-
Ujjerezet-	DNS-
Tenyérerezet-	Arc és alak-
Test hőkép-	Szag azonosítók, stb.

A biometrikus azonosítást már világszerte alkalmazzák, elsősorban beléptető rendszereknél, ahol a megbízhatóság alapját a nem átadható adat jelenti, így sem elveszíteni, sem ellopni nem lehet. Biometrikus azonosítónkat mindenhova magunkkal visszük, az olvasó szerkezetek kezelése pedig általában mindenki számára rendkívül egyszerű. Az azonosítás biometrikus formájának további alkalmazási lehetőségeiről a következő fejezetemben kívánok szót ejteni.

Fontos megemlíteni a biometrikus azonosítás biztonságának kérdését, amelyhez az FAR (False Accept Rate) illetve az FRR (False Reject Rate) mutatókat használjuk, magyarul Téves Elfogadás illetve Visszautasítás. [1]

FAR = Megmutatja, hogy az azonosítás milyen arányban ismert fel jogosulatlan felhasználót jogosultként.

FRR = Megmutatja, hogy az azonosítás milyen arányban utasít el jogosult felhasználót.

A pontosság az FAR és FRR értékgörbék metszéspontja, amely az EER (Equal Error Rate) érték. Néhány példa a rendszerek pontosságára (EER): [2]

- Hangazonosítás: 1 : 50
- Ujjnyomat azonosítás: 1 : 500
- Írisz azonosítás: 1 : 131.000
- Retinaazonosítás: 1 : 10.000.000+

A biometrikus azonosítás megfelelő formáját kiválasztva, ahogy a személyazonosítási eljárásokat elemeztük, láthatjuk, hogy egy rendkívül megbízható azonosítási módszerhez juthatunk, amely ténylegesen magát a személyt azonosítja. A biometria sok előnyén túl, hátrányokkal is számolnunk kell: [3]

- a módszerek legtöbbje rendkívül költséges, drága hardvert igényel,
- higiéniai szempontból a fizikai kontaktust igénylő megoldások problémásak,
- fogyatékkal élők számára egyes eljárások nem alkalmazhatóak,
- egyes fizikai jellemzők az idő múlásával vagy betegség következtében változhatnak, stb.

3. AZ AZONOSÍTÁS MÓDSZEREI

A korábbiakban csak felsorolás szintjén említett biometrikus azonosítási eljárásokból a fontosabbakat jelen fejezetben röviden kerül ismertetésre, külön részletesen kitérve az ujjnyomat azonosítás technikájára.

3.1. Biometrikus azonosítási módszerek

Tenyérnyomat azonosítás: A tenyérnyomat azonosítás nem egy általánosan használt biometrikus azonosítási forma, elsősorban bűntettek helyszínén lelhető fel. Azonosításukkor általában a tenyéren található fővonalak ráncolatát, a fodorszálakat illetve a szövetmintázatot elemzik, amelynek során gondos munkát követően az ujjnyomathoz hasonlóan jellegzetes információhordozót kaphatunk. (1. ábra) [4]

1. ábra. Tenyérnyomat azonosítás;
Forrás: http://www.chs81.com/sitebuildercontent/sitebuilderpictures/401pray/handprint.jpg;
http://stepintoyourlight.com/wordpress/wp-content/uploads/2009/11/Left-hand-print-244x300.jpg;
(2011. 09. 15.)

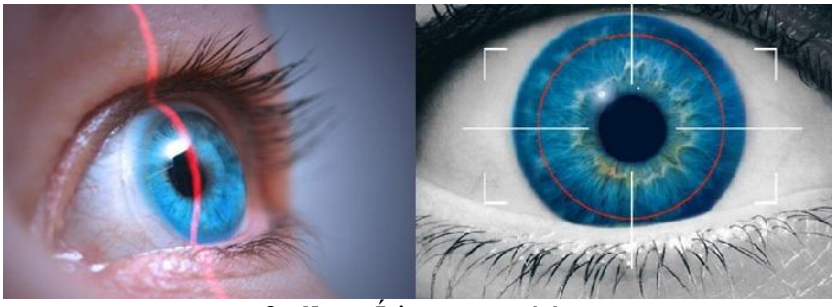
Kézgeometria azonosítás: A tenyérnyomatnál gyakrabban alkalmazott azonosítási eljárás, amelynek gyors leolvashatósága illetve pontossága adja előnyét. Működésének lényege, hogy a kéz felületéről és formájáról vesz mintát, és azt analizálja, így figyelembe veszi az ujjak hosszúságát és szélességét, a kézfej szélességét, illetve a tenyér és az ujjak méretarányát. A hatékony felismerést négy pozícionáló tüske segítségével érik el, amely azonos állásba helyezi a tenyeret a beolvasáshoz. Léteznek pozícionáló tüske nélküli felismerők is, ezek különböző sajátos értékeket elemeznek. Széles alkalmazási területtel rendelkezik, például munkaidő nyilvántartási rendszerek. Nagy előnye hogy más rendszerekkel is könnyen integrálható. [4] [5]

Ujj- és tenyérerezet azonosítás: Az ujj- és tenyérerezet azonosítás egy viszonylag új módszer a biometrikus azonosítás terén. A két módszer között lényegi különbség nincs, csak az eszköz más. A működés alapja, hogy az ujjat vagy tenyeret infravörös fénnyel megvilágítják, ami a különböző szövetekről a különböző szintű elnyelődés miatt, más intenzitással verődik vissza. Az érhálózatban lévő vér sokkal jobban elnyeli a fényt, így az szemmel látható módon kirajzolódik az eszköz számára. Az érhálózatokat más biometrikus azonosítási eljárásokhoz hasonlóan, jellegzetességeik alapján mérik. Előnyei közé tartozik, hogy nem befolyásolja felszíni sérülés, illetve szinte lehetetlen hamisítani. (2. ábra) [4] [6]

2. ábra. Tenyér érhálózat (bal) és ujj érhálózat olvasó (jobb)
Forrás: http://cache.gizmodo.com/assets/images/gizmodo/2008/07/palm-vein-scan.jpg; http://img.directindustry.com/images_di/photo-g/biometric-sensor-finger-vein-reader-396431.jpg

Írisz azonosítás: A szem szivárványhártyáján alapuló biometrikus azonosítás egyike a legjobb azonosítási módoknak, köszönhetően az akár 400 azonosítható jellemzőnek, amely segítségével a tévedés lehetősége minimálisra csökken. Az írisz életünk során nem változik, így az eljárás megbízhatósága nő. Annak az esélye, hogy két írisz megegyezzen, szinte kizártnak tekinthető, mivel az eljárás pontossága több mint 10^{70} nagyságrendbe esik.

A vizsgálat során a szivárványhártya látható és láthatatlan tulajdonságait elemzik. A látható közé tartozik az írisz sugaras mintázata, a körökkel, árkokkal és a koronával, a láthatatlan pedig az infravörös leolvasás során láthatóvá váló retinahártya erezet. Leolvasás során aktív illetve passzív felvételkészítésről beszélhetünk. Az aktív során a kamerához közel kell tartani a szempárját, míg passzív esetében a kamera az, ami bepozícionálja a szempárt. Az írisz azonosításon alapuló technika nagy hátránya, hogy a berendezések rendkívül bonyolultak, így áruk is magas. (3. ábra) [4] [7]



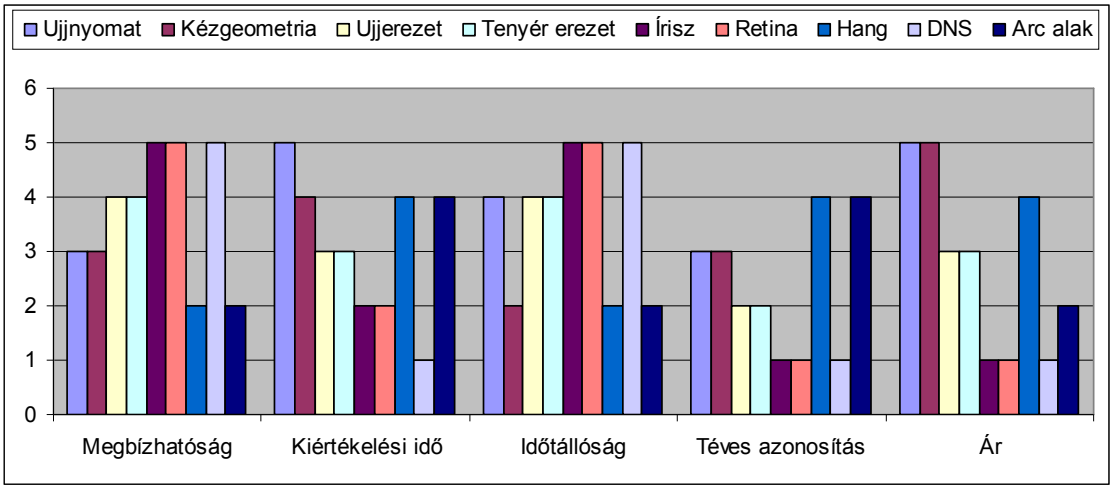
3. ábra. Írisz azonosítás

Forrás: http://www.airport-int.com/upload/image_files/articles/images/companies/1688/biometrics-sec01-l.jpg; http://fingerprint-security.net/wp-content/uploads/2011/05/Iris-Scan.jpg

Retina azonosítás: A retina alapú azonosítás során infravörös fénnyel világítják meg a szemfenéken található retinát, így az ujj- és tenyérerezet azonosítóhoz hasonlóan működve, az infrasugarak eltérő mértékben nyelődnek el, kirajzolva a szemfenék érhálózatát. A módszer egyik legnagyobb hátrányát jelenti, hogy a mintavételezési eljárás során az olvasóval közvetlen kapcsolatot kell kialakítania a szemnek, ami által nő a fertőzésveszély. Ilyen technológiát csak rendkívül ritkán alkalmaznak, általában nagy biztonságot igénylő helyszíneken. [8] [9]

DNS azonosítás: A DNS azonosítás eltér az eddig elhangzott azonosítási módszerektől, mivel a gyakorlati életben nem használható. Az eljárás egyrészről rendkívül időigényes, mivel nagyon bonyolult laborvizsgálatok szükséges elvégezni, másrészről egy emberi DNS bárhonnan beszerezhető, így akár egy hajszálból is másolható.

Az alábbi diagramom (1. Diagram) a különböző biometrikus azonosítási módszerek egyes tulajdonságainak értékelését kívánja bemutatni, 1-5-ig tartó skálarendszerben. Az 5-ös érték jelenti a legjobbat, az 1-es a legrosszabbat.



1. diagram. Biometrikus azonosítási módszerek tulajdonságainak értékelése

3.2. Az ujjnyomat azonosítás

Mielőtt ismertetném az ujjnyomat azonosítás technikáját, nézzük meg hogy pontosan mit is jelent az ujjnyomat. A daktiloszkópia három féle ujjról származó mintát különböztet meg:

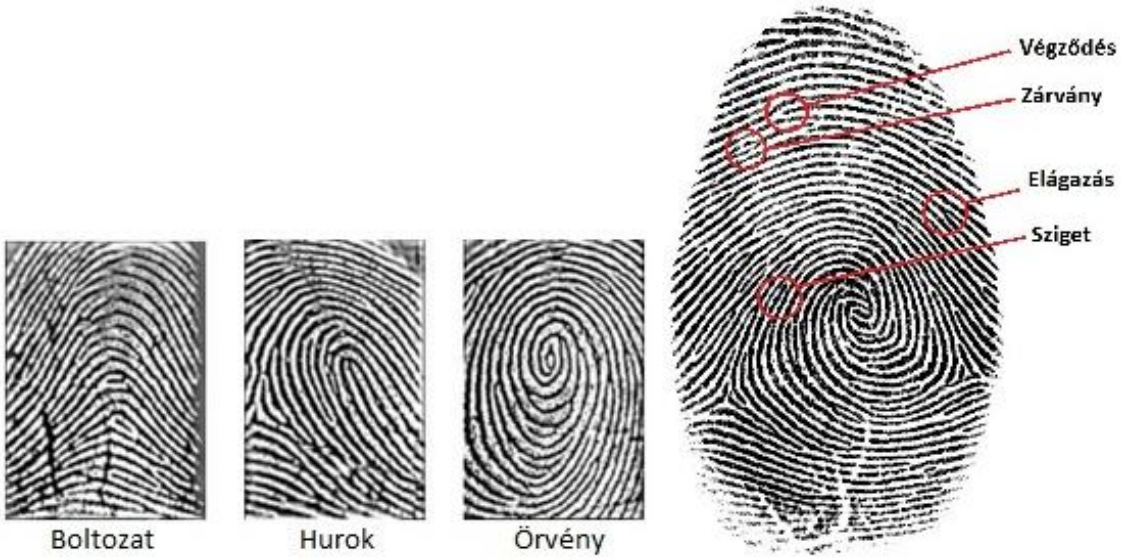
Ujjnyom: Azokon a tárgyakon lelhető fel, amiket az ember megérint. Általában rossz minőségű képet adnak.

Ujjlenyomat: Az ujjról készült jó minőségű képek, amelyek az ujjvégi ujjperc teljes, körömtől-körömig tartó lenyomatát képezi. Általában rendőrségi nyilvántartásokban használják.

Ujjnyomat: A síkfelületre helyezett ujj ott maradó, kétdimenziós lenyomata. Általában jó minőségű, a személyazonosításban használatos, a továbbiakban erről lesz szó. [16]

Az ujjnyomat azonosítási technika kulcsa, hogy az ujj barázdáltsága mindenkinek egyedi mintázatú. A mintázat 18 hetes korunkban alakul ki, és a későbbiekben sem változik, követi a kéz méretbeli változását. Az égés, vágás, kopás vagy marás során keletkező sebesülések 10-40 napon belül képesek regenerálódni. [17] Az ujjunkra tekintve láthatunk kis barázdákat, vonalakat, amelyeket fodor szálnak illetve fodor vonalnak nevezünk. A fodor szálak az ujjnyomat globális és lokális jellemzőit határozzák meg.

A *globális jellemzők* (4. ábra) a fodor vonal minták, amelyek három nagy csoportot alkotnak: [10] [12]



4. ábra. Globális és lokális ujjnyomat jellemzők

Boltozat: A barázdák az egyik oldalról a másik oldalra szinte egyenes vonalban, vagy boltozatot rajzolva haladnak át.

Örvény: A barázdák egy mag körül kör, spirális vagy ovális mintát követve rajzolódnak ki.

Hurok: A barázdák belépnek az ujjnyomat minta területére, majd a mag körül visszagörbülnek és a belépési vonalhoz közel hagyják el a minta területét.

A globális jellemzők relatív gyakorisága eltérő, a boltozaté 3%, az örvényé 25%, a huroké pedig 72%. [12]

A *lokális jellemzők* (4. ábra) a minuciákhoz kapcsolódnak. A minuciák nem mások, mint a barázdák jellegzetes mintái, ezek azok a tulajdonságok, amik nem egyeznek meg az embereknél. Ezeknek néhány jellemző típusai: Elágazás, híd, pont, sziget, kereszteződés, kettős híd, végződés, horog, oldalkontaktus, kettős elágazás, áthaladó vonal, stb. [13]

Az ujjról származó lenyomat azonosítás régóta ismert és használt módszer, már 1902-ben is alkalmazták a kriminalisztikában. A teljes ujjlenyomat kb. 100 jellegzetes minucia pontot tartalmaz, az ujjnyomat azonosítók pedig általában 60 minucia pontot hasonlítanak össze egy adott mintáról. A jelenleg használatos ujjnyomat olvasó rendszerek között jelentős különbségek lehetnek az olvasási technológia vagy a költségek szempontjából.

Nézzük át az ujjnyomat olvasási technikákat:

3.3. Ujjnyomat olvasó rendszerek

Az ujjnyomatok olvasására sokféle technikai megoldás létezik, a rendőrségi módszeren keresztül egészen az ultrahangos leolvasásig. Egyes ujjnyomat azonosítók képesek megvizsgálni, hogy az ujj élő-e, ezt pedig az ujj hőmérsékletének és\vagy nedvességtartalmának elemzésével végzik el. Az ujjnyomat azonosító eszközök közötti

hasonlóság, hogy mindegyik az ujjakon lévő fodor szálak egyediségét elemzi, tárolja le, és hasonlítja össze az azonosítandóval. (5. ábra)

5. ábra. Ujjnyomat olvasó rendszerek
Forrás: http://fingerprint-security.net/wp-content/uploads/2011/07/fingerprint-scan.jpg; http://www.procontrol.hu/GyartasFejlesztes/Termekeink/ProxerBio2/proxerbio_300.jpg

A különbség az olvasási technikákban van. Az olvasás alapvetően lehet optikai, illetve egyéb, nem optikai módszer.

Optikai elvű képfelvételek: [4] [14] A feldolgozandó ujjnyomatot egy képbontó eszköz felületére képezzük le egy optikai rendszer segítségével. A képbontó eszköz CMOS vagy CCD elem.

- Totálreflexiós: Az ujjunkat egy prizma felületére helyezzük, majd a megvilágítás során a kép egy képbontó eszköz felületére képződik le.
- Diffrakciós: A totálreflexióshoz hasonló működés, de prizma helyett fresnel lencsét alkalmazunk.
- Chip-szenzor: A szenzor felületére helyezzük az ujjunkat, a feldolgozandó információt pedig optoszálak vezetik a képbontó eszközre.
- Termikus elemzés: Az ujjnyomat olvasó érzékelőjéhez nem kell hozzáérni, csupán elhúzni az ujjat, amit szeletenként olvas le és alkotja meg a képet. A szenzor a bőr barázdáinak hőmérsékleti különbségét érzékeli.

Nem optikai elvű képfelvételek: [4] [14] Valamilyen egyéb, nem optikai elven működő eszközzel kerül az ujjnyomat beolvasásra.

- Rádiófrekvenciás elv: Rádiófrekvenciás jelet juttatunk az ujjra, amely azt visszasugározza a vevőantennaként szolgáló szenzor felületére. A rádiófrekvenciás jel, képes mélységi képet is alkotni az ujjunkról és barázdáiról.
- Kapacitív elv: Az apró kondenzátorokkal rendelkező szenzor felületére helyezzük az ujjunkat, amely eltérő kapacitást mutat a barázdák és a köztes völgyek függvényében. Az eltérő kapacitás kerül elektromos jellé alakítva kiértékelésre.
- Ultrahangos elv: A szenzor ultrahangot sugároz az ujjra, amelyről visszaverődő hullámokból mélységi képet alkot.
- Nyomásérzékelős elv: A szenzor felülete alatt piezo-elektromos nyomásérzékelő mátrix helyezkedik el, amely az ujjfelület egyenetlenségeit érzékelve alkot képet.

4. ALKALMAZÁSI LEHETŐSÉGEK

A biometrikus azonosítás már nem a jövő gondolata. Elegendő olyan mindennapi dolgokra gondolni, mint az új útlevelek, egyes laptopok és mobiltelefonok, és láthatjuk, hogy széles körben egyre gyarapszik a biometrián alapuló azonosító rendszerek felhasználási köre. A biometrikus azonosítási eljárásról már kijelenthetjük, hogy az a technológia, ami 15 évvel ezelőtt a távközlés, 10 évvel ezelőtt pedig az internet volt. A biometria egy olyan új technológia, amely rohamos ütemben fejlődik, és az élet egyre több területén fog aktívan jelentkezni.

A rohamos elterjedés mögött mind a kereslet, mind a kínálat szerepel. A keresleti oldalon megvan az igény a biztonságra. Az államok szeretnék tudni kik lépik át határaikat, a cégek pedig szeretnék tudni kik lépnek be épületeikbe. A kínálat oldalán pedig megjelennek a rendkívül kompakt és olcsó eszközök, amik könnyedén beépíthetőek bármilyen eszközbe.

Az emberek az új technológiát egyre elfogadottabbnak tartják, egyre gyakrabban alkalmazzák laptopjuk vagy telefonjuk védelmére, külföldön pedig már széles körben alkalmazzák jelenleg is, íme néhány példa:

- Chicago: A biometrikus fizetés lehetőségét tesztelik az autósok. Bizonyos benzinkutakon már ujjnyomattal is fizethetnek, az ujjnyomat érzékelős készülékek az autósok bankszámlájához kapcsolódnak, így a fizetés onnan történik. [15]
- Japán: Ujjnyomat érzékelős pénz automatákat alkalmaznak bizonyos bankok ATM rendszerei, pénzfelvétel céljára. (6. ábra) [16]
- Florida: Disney World-ben a beengedő kapuknál minden látogatótól ujjnyomatot vesznek és társítják a belépőkártyájukhoz. [15]
- Nagy-Britannia: Írisz felismerésen alapuló beléptető rendszer a nagyobb repülőtereken a gyakran visszatérő látogatók számára. [17]
- Egyesült Államok: 1996 óta alkalmaznak egyes büntetés végrehajtó intézményekben írisz felismerésen alapuló rendszert a rabok nyilvántartására. [18]

6. ábra. Ujjnyomat érzékelős ATM
Forrás: http://www.itcbd.com/wp-content/uploads/2010/09/Biometric-Solution.jpg;

Talán a legjobb példa a biometrián alapuló azonosítási rendszerek széles körű alkalmazására, az Egyesült Államok bevándorlási hivatalának rendszere. A rendszer a belépő személyek ujjnyomatát hasonlítja össze az adatbázisában szereplő több mint 2,5 millió azonosítójával. 2004-es bevezetése óta több mint 75 millió látogató ment keresztül a rendszeren, és körülbelül ezer alkalommal tagadták meg a belépést. [15]

A biometrikus azonosítás nem más, mint a jövő a jelenben. Lássunk néhány lehetséges felhasználási területét a biometrián, azon belül is az ujjnyomat azonosításon alapuló rendszereknek:

- Bank automaták szolgáltatásai: Ahogy más országokban már napjainkban is sikeresen működik, úgy hazánkban is várhatóan meg fog jelenni a bankkártya nélküli biometrikus azonosításon alapuló bank automata használat.
- Személyazonosítás: Mindenhol alkalmazhatóvá válik a biometrikus azonosítás módszere, ahol jelenleg is igazolnunk kell magunkat.
- Munkaidő nyilvántartás: Munkahelyünkön a munka megkezdése egy biometrikus azonosítással történik, ahogy a munkahelyünk elhagyása is, ezzel máris kiküszöbölhető a munkaidő eltitkolt rövidítése.
- Kasszánál történő fizetés: Bankkártyánk helyett elég ujjnyomatunkat használnunk, és a kasszánál történő fizetés gyorsabb és biztonságosabb is lesz.
- Belépés azonosítás: Munkahelyre történő belépés során biometrikus azonosítónkkal igazoljuk magunkat és jogosultságunkat a belépésre.
- Csekkbeváltás: Nem szükséges igazolvány hordása, elegendő az ujjnyomatunk használata.
- Otthoni biztonsági rendszer: Vagyonvédelmi rendszerünket, vagy intelligens otthonunkat nem kell kóddal aktiválni, biometrikus azonosítónk alapján felismer minket, a vagyonvédelmi rendszert iktatja, az intelligens épület automatika pedig előre meghatározott módon jár el.
- Bankkártya biztonság: A kód elleshető, kitalálható, ujjnyomatunk azonban csak kikényszeríthető, a kettő együttes alkalmazása viszont biztonságot adhat.
- Elektronikus fizetés: Elektronikus formában történő fizetés esetén elegendő egy géphez csatlakoztatható ujjnyomat azonosító, és a hitelesítés a jelszón túl már nagyobb biztonságot nyújt.
- Elektronikus hozzáférés: A fizetéshez hasonlóan hitelesít minket biometrikus azonosításunk alapján.
- Részvétel ellenőrzés: Kötelező részvétel esetén nem játszható ki az ujjnyomat olvasó rendszer, ott kell lennünk személyesen.
- Utazás szabályozás: Országok határait átlépve azonosíthatjuk magunkat, repülőgépes utazás során rendkívül hasznos.
- Távoli szavazás: Hazánkon kívül is leadhatjuk voksunkat egyszerűen azonosítva magunkat.
- Automata eszközműködtetés: Az intelligens otthont megteremtve, az automatizált gépeket, ujjnyomatunk alapján felprogramozhatjuk tevékenységekre.
- Jogosultság ellenőrzés: Például gépjárművek esetében központi ellenőrzés a jogosítvány meglétére.
- Szerver biztonság: Hitelesség ellenőrzése biometrikus azonosság alapján.
- Stb.

Az említett lehetőségek csupán néhányak a sok közül, hiszen az ujjnyomat azonosításon alapuló technikák mindenhol alkalmazhatóak ahol fokozott biztonságra van szükség, vagy ahol a mindennapi életben is szükséges személyazonosságunk igazolása, illetve kártyák és jelszavak, PIN kódok alkalmazása. [19]

4.1. Felmérések és vélemények

Kutatásom során sikerült a magyar lakosság véleményalkotásáról is képet kapnom. A felmérést a Polygon Informatikai Kft. készítette, kizárólag tájékoztató jelleggel kívánom bemutatni. A felmérésen 548 fő vett részt, akik 18 és 60 év közötti lakosok.

A felmérés négy kérdésből állt, amelynek során a biometrikus azonosítási eljárások ismertségét vizsgálták. A válaszadók 85%-a hallott már ilyen típusú azonosítási eljárásról, de mindössze 13%-uk találkozott már vele. A válaszadók jelentős része filmekből vagy híradásokból tájékozódott a technikáról. Bár a résztvevők nagy részének véleményalkotása

nem a személyes tapasztalaton alapszik, mégis csak a megkérdezettek 16%-a mondta, hogy soha nem vennék rá alkalmazására.

A lakosság jelentős része tehát kész befogadni és alkalmazni a biometrikus azonosítási technikákat, elsősorban olyan helyeken, mint a határforgalom, banki ügyintézés, vásárlás vagy hivatalos ügyek intézése, annak ellenére is, hogy többségük még nem használta soha, vagy nem rendelkezik róla mélyebb tudással. [20]

4.2. Biometriával kapcsolatos aggodalmak

Bár a biometrikus eljárások a szakértők véleménye alapján is biztonságosnak tekinthetők, nehezebb feltörni őket, de nem szabad megfeledkeznünk róla, hogy ezeknek a rendszereknek is vannak gyenge pontjai. Jelen dolgozatomban nem kívánok részletesen foglalkozni a biometrikus azonosítási technológiák veszélyforrásaival, azonban az alapvető aggodalmakat meg szeretném említeni.

Az általam feldolgozott források és tanulmányok alapján kijelenthetem, hogy az emberek aggodalma két fő csoportba osztható:

Az egyik a biztonság, amely a támadástól vagy feltöréstől való félelem. A biometrikus rendszerek feltörésének valós veszélyei vannak. A rendszerek legsebezhetőbb pontjai pedig a háttér adatbázisok, és a csatornák, amelyek a rendszer egyes elemeit összekötik. Biometrikus és kriptografikus módszerek okos kombinációival azonban megakadályozható, hogy ezeknek a rendszereknek az adatait a hackerek lehallgassák, továbbítsák vagy módosítsák.

A félelem másik forrása, a visszaélés, amelynek során az állam vagy a hatósági személyek visszaélnének adatainkkal és azt nyomon követésre használnák.

A fent említett két félelemforrás megfelelő törvényi szabályozással, odafigyeléssel és a kételyek eloszlatásával orvosolható, azonban figyelembe kell venni, hogy egyes emberek vallási alapon nem lennének hajlandóak használni az eszközöket.

Az aggodalmak ellenére a biometriai technológiák fejlődése megállíthatatlan, hisz egyrészről kényelmet, másrészről biztonságot nyújtanak az embereknek, és szinte biztosan állítható, hogy a jövőben egyre gyakrabban fogunk találkozni a személyazonosítás biometrikus lehetőségével.

5. ÖSSZEGZÉS

A biometrikus azonosításon alapuló technológiák az utóbbi éveket megfigyelve rendkívül gyors tempóban fejlődnek és terjednek el széles felhasználási körben. Ez a folyamat pedig megfelelő odafigyeléssel és adatvédelmi szabályozással egybekötve pozitív hatással, megkönnyítve hathat az emberek mindennapi életére. A biometrikus azonosítás a jövőben mind hétköznapibbá fog válni, és idővel nem lesz szükségünk semmilyen azonosító eszközre, csak személyes jelenlétünkre. Bár a hagyományos azonosító eszközök teljes felváltása a közeli jövőben még nem lehetséges, de valószínűsítem, hogy a bank automatától kezdve egészen a hivatali ügyek intézéséig minden biometrikus azonosítással fog történni. A világ a biometrikus azonosításnak köszönhetően meg volt változni, ez feltartóztathatatlan, a megfelelő használat azonban elsősorban tőlünk, emberektől függ.

Felhasznált irodalom

[1] [1] Bromba Biometrics: Biometrics FAQ, http://www.bromba.com/faq/biofaqe.htm; (2011. 09. 10.)

[2] Biometriai alapelvek, http://www.slideshare.net/szabojudo/biometriai-alapelvek; (2011. 09. 10.)

[3] Biometrián alapuló azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=143; (2011. 09. 13.)

[4] Dr. Kovács Tibor: Biometrikus azonosítás, Főiskolai digitális jegyzet, BMF, Budapest, 2009.

[5] Kézgeometria, http://handyman.hu/szakkifejezesek/kezgeometria/; (2011. 09. 15.)

[6] Vein Recognition Biometrics, http://www.findbiometrics.com/vein-recognition/; (2011. 09. 17.)

[7] Írisz azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=149; (2011. 09. 17.)

[8] Retina azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=148; (2011. 09. 20.)

[9] Retina azonosítás, http://www.recoware.hu/biometria/biometriai_azonositas/biometriai_azonositasi_modszerek_felsorolas_retina.html; (2011. 09. 21.)

[10] Ujjnyomat alapú azonosítás, http://www.biztostu.hu/mod/resource/view.php?id=144; (2011. 09. 25.)

[11] Bunyitai Ákos: A ma és a holnap beléptetőrendszereinek automatikus személyazonosító eljárásai, Hadmérnök, VI. évfolyam, 1. szám, 2011

[12] Ujjnyomat azonosítás, http://sdt.sulinet.hu/Player/Default.aspx?g=9ef262fa-640b-4977-a546-43ef6613adaa&cid=d719a68c-3bea-46ce-9f54-dca11d4f8e9c; (2011. 10. 10.)

[13] Daktiloszkópia, http://www.biztostu.hu/mod/resource/view.php?id=145; (2011. 10. 13.)

[14] Ujjnyomat érzékelés technikák, http://oktel.hu/szolgaltatas/belepteto-rendszer/biometrikus-azonositas/; (2011. 10. 13.)

[15] Jövő már a jelenben, http://www.origo.hu/tudomany/20071105-biometrikus-azonositas-jovo-mar-a-jelenben.html?pIdx=1; (2011. 10. 15.)

[16] Ujjnyomat a kézpénzfelvételhez, http://www.digibiz.hu/elegendo-egy-ujjlenyomat-a-keszpenzfelvetelhez/20100604; (2011. 10. 17.)

[17] Írisz felismerés, http://www.nagyutazas.hu/magyar/utikalauz/article.php?id=557&no_results_total=80&lstresults=3; (2011. 10. 17.)

[18] Iris recognition, http://ntrg.cs.tcd.ie/undergrad/4ba2.02/biometrics/now.html; (2011. 10. 17.)

[19] Future of biometrics, http://www.optel.com.pl/article/future%20of%20biometrics.pdf; (2011. 10. 20.)

[20] Felmérés, http://www.hwsw.hu/hirek/31920/biometrikus_azonositas_felmeres.html; (2011. 10. 20.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Gávay György
gavay.gyorgy@uni-nke.hu

AZ LPG ALKALMAZÁSÁNAK LEHETŐSÉGEI A MAGYAR HONVÉDSÉG GÉPJÁRMŰTECHNIKAI ESZKÖZEIBEN ALTERNATÍV TÜZELŐANYAGKÉNT

Absztrakt

A XXI. század elején egyértelművé vált az energiaigény biztosításának nehézsége szinte minden területen. Minden hadsereg fenntartó szervezete keresi a megoldást a költségek csökkentésére, illetve arra, hogy mindennapi működés, és feladatellátás a legkisebb kárt okozza a környezetben. Minden ötletet érdemes megvizsgálni a lehető legtöbb szempontból, és az arra érdemes gondolatokat akár tudományos részletességgel kielemezni. Egy alternatív tüzelőanyag alkalmazása együtt jár számos más problémával, melyre megoldást kell keresni. Ha a logisztikát, és az okmányolást érintő megoldások kidolgozásra kerülnek, lehetőség adódik egyes eszközök gazdaságosabb, környezettudatosabb üzemeltetésére.

At the beginning of the 21st century the difficulties of ensuring energy needs became obvious in almost every field. All military maintenance organizations are searching for a solution to cut the costs and to guarantee that the everyday operation and functions do the least possible harm in the environment. It is worth to examine the ideas from all possible angles and the best theories may also be analyzed in a scientific way. The usage of an alternative fuel comes together with numerous problems that need to be solved. If the solutions concerning logistics and documentation get worked out, there will be a chance to operate the vehicles in a more profitable and environmentally conscious way.

Kulcsszavak: *alternatív tüzelőanyag, LPG, etanol, kettős tüzelőanyag-rendszer, rendszerben tartás ~ alternative fuel , Liquified Propane Gas, ethanol, dual fuelsystem, keeping in system*

1. BEVEZETÉS

A Magyar Honvédség gépjármű-technikai haditechnikai eszköz állománya szinte kivétel nélkül belsőégésű motorral hajtott eszközökből áll. Az eszközök üzemeltetésében az elsődleges prioritás a hadra fogható állapot fenntartása, de nem szabad megfeledkeznünk a gazdaságos és környezetbarát üzemeltetés fontosságáról sem. Minden olyan területet érdemes megvizsgálnunk, amely nem jár a hadrafoghatóság veszélyeztetésével, de lehetőséget biztosít a fent említett tudatos üzemeltetésre.

Az eszközök fejlesztése természetesen folyamatos, de a lehetőségek korlátozottak. A modernizáció két lehetséges útja, az eszközök megvásárlása, rendszerbe állítása, illetve a már rendszerben lévő eszközök korszerűsítése. Az eszközök fejlesztése természetesen azok felhasználási területe szerint történik, és ha ez a fejlesztés az üzemeltetést érintő módosításokat jelenti, akkor az eszköz teljes üzembentartási rendszerét érinteni fogja.

A cikk egy alternatív tüzelőanyag alkalmazásának lehetőségét vizsgálja a Magyar Honvédségen belül. Első lépésként meg kell vizsgálni a felmerülő lehetőségek nyilvánvaló előnyeit és hátrányait. Logisztikai szempontok szerint a legelőnyösebb egyetlen univerzális tüzelőanyag használata. A tárolási, szállítási és gazdálkodási feladatok, azaz az ellátás és az utánpótlás problémái műveleti területen megkerülhetetlenek. Ezeket bonyolítani, szerteágazóvá, nehezen átláthatóvá és nehezen tervezhetővé tenni egyértelműen nem lenne helyes. Dízel üzemű eszközök esetében már olyan tényekkel kell szembenéznünk, amelyek alapvetően behatárolják a vizsgálat irányát, a motor működése ritkán ad lehetőséget a tüzelőanyag alternatív helyettesítésére[1].

Műveleti területen a feladatellátás, az élőerő, illetve az eszközök megóvása minden más szempontot felülír. Béke területen a logisztikai szállítási feladatok, az információ áramoltatási, irányítási, és tervezési feladatokhoz igénybe vett eszközök üzemeltetési körülményei már lehetőséget engednek az alternatív tüzelőanyagok alkalmazásának vizsgálatára. Ez esetben is külön kell vizsgálni az eszközöket a felhasznált tüzelőanyag szerint:

- Benzinüzemű eszközök esetén az alternatív tüzelőanyag-ellátást biztosító rendszerek kiépítése nem zavarhatja meg az eszköz eredeti, saját tüzelőanyag-ellátó rendszerének működését. Olyan megoldásokat lehet felsorolni, melyeket a magyar ipar, illetve kereskedői hálózat biztosítani képes. Alternatív tüzelőanyagokra három lehetőség nyílik:
  - *a)* Etanol
  - *b)* LPG [10]
  - *c)* CNG
- Dízelüzemű eszközök tekintetében már csak jelentős átalakítással járó, az eredeti tüzelőanyag-ellátó rendszer cseréjével lehet megoldást találni, illetve a Dízel-LPG[2] vegyes üzemeltetés jöhet szóba.

[1] A Magyar Honvédségben rendszeresített T-72-es harckocsik motorja több tüzelőanyaggal is üzemeltethető, de alapvetően dízelüzemű motorokról van szó.

[2] A közúti szállítás költségeit lehet számottevő mértékben csökkenteni, az említett módszerrel, de jelentős költségeket jelent az átalakítás. Ausztráliában több évtizedes múltra tekint vissza, míg Európában, napjainkban került előtérbe a technológia fejlesztésének kérdése.

2. A TÜZELŐANYAGOKRÓL RÖVIDEN

A tüzelőanyagok összetétele többek között az égés sebességét, az égéstermékek összetételét, és ezzel a motor termikus, kémiai és mechanikai igénybevételét határozza meg. [2] A megbízható motorműködéshez olyan tüzelőanyagot [8] kell választani, amely minden szempontból – lehetőleg gazdasági szempontból is – előnyös legyen.

A mai környezetvédelmi előírások jelentősen kihatnak a tüzelőanyagok adalékolására.[3]

2.1. Az Etanol

Az etanol (C_2H_5CH) alkalmazása tüzelőanyagként világszerte folyamatosan terjed. Dél-Amerikában az éghajlati viszonyok kedvezőek a cukornádtermeléshez, így jelentősen olcsóbban előállítható nagy mennyiségben ez a szénhidrogén. Brazíliában 1981 óta minden állami személygépkocsi 100% etanollal üzemeltethető, és már 1985-től elterjedt a 20/80%-os alkohol-benzin arányú tüzelőanyag használata [1]. Sajnos Európában csak jelentős adókedvezmények árán biztosítható a versenyképes piaci ár. Neves autógyárak fejlesztenek etanol vagy benzin-etanol vegyes üzemű típusokat. Az utólagos átalakítás nem igényel nagy befektetést, de sajnos nem építhető ki párhuzamos tüzelőanyag-ellátó rendszer. Egy jól beállított, etanol üzemhez átalakított gépjármű a benzin-etanol 15-85% - os térfogatarántól a 100-0%-os összetételig szinte kifogástalanul működik, leszámítva a jelentős többletfogyasztásból adódó, az igénybevétel tervezésével járó problémákat és a sűrűn előforduló hidegindítási nehézségeket, illetve a tüzelőanyag ellátó rendszer esetleges meghibásodásait. A járművek tüzelőanyag-ellátó rendszereit a tüzelőanyag tartálytól kezdve –

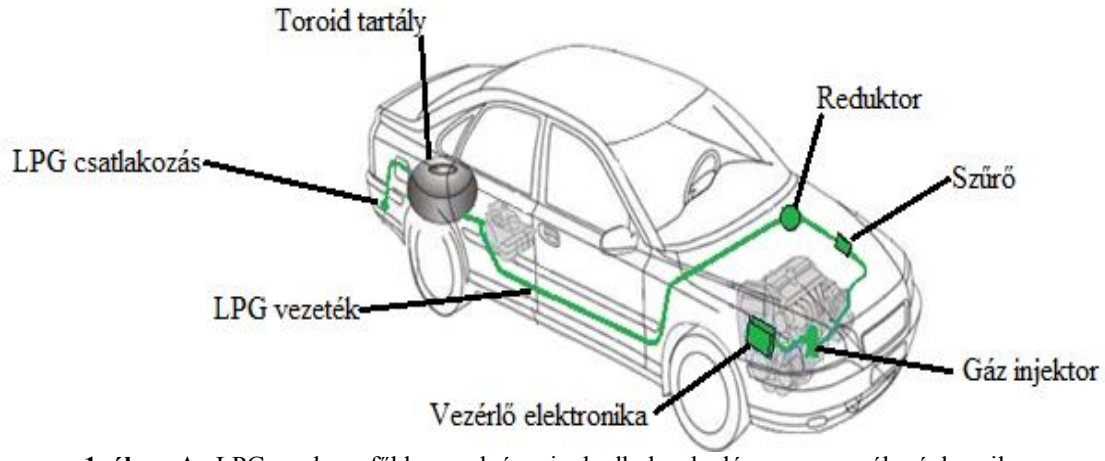
a tápszivattyút és a vezetékeket is beleértve – egészen a befecskendező elemekig úgy tervezik meg, hogy adott tüzelőanyag fajta követelményeinek megfeleljen. Sajnos egy nagy futásteljesítményű gépjármű esetén a tüzelőanyag megváltoztatásának következményei nem prognosztizálhatóak. Az alkohol bizonyos könnyűfém-ötvözetekben, illetve tömítésekben is kárt tehet, nem beszélve jelentős vízmegkötési tulajdonságáról, mely miatt nem csak a tüzelőanyag szűrő, hanem más részegységek is képesek eltömődni. Amennyiben a tüzelőanyag-töltő állomás tartályából – bármilyen okból kifolyólag – nagyobb mennyiségű víz kerül a tüzelőanyag-ellátó rendszerébe, úgy a rendszer tisztítása elkerülhetetlenné válik, és egy korszerű jármű esetében ez jelentős javítókapacitást vesz igénybe.

Az átalakított járművek tárolása [7] nem jelent megoldhatatlan problémát, mert az egyetlen komoly különbség, hogy az etanol tiszta, halvány, kékes lánggal ég jellemzően koromképződés nélkül. A telephelyen, illetve tárolóban egy esetleges tűz gyors lokalizálását teszi nehézzé ez a körülmény. Bár az eszközök tüzelőanyag-ellátása csak a gazdasági szempontok figyelembevételével válik körülményessé, a tüzelőanyag-fogyasztás oly mértékben függ annak összetételétől (benzin-etanol arány), hogy az igénybevételre való tervezés ellehetetlenül. Ez esetben még a gazdasági számításokkal sem érdemes foglalkozni.

3 A katalizátorok megjelenése és a környezetvédelmi normák szigorodásának együttes hatására az ember és a környezet számára is mérgező ólom-tetraetil Pb(C2H5)4 alkalmazása megszűnt, mivel a katalizátort nagy mértékben károsítja [4]

2.2. LPG (Liquified Propane Gas)

Alkalmazása több évtizedes múltra tekint vissza. A benzin-gáz üzem alapja, hogy nem befolyásolja a jármű benzinnel való üzemeltetését.



1. ábra. Az LPG rendszer főbb szerelvényeinek elhelyezkedése egy személygépkocsiban

Az LPG cseppfolyósított PB[4] – propánbután – gáz, amely tulajdonságait az MSZ EN 589 szabvány határozza meg. Számos szempontból előnyösebb tulajdonságokkal bír, mint a benzin. Kevesebb lehet benne a szennyeződés és nem tartalmazhat vizet. A PB gáz gyakorlatilag a szénhidrogén-bányászat és a kőolaj-feldolgozás melléktermék, melyet háztartási és fűtési célokra értékesítenek.

A PB gáz tárolása cseppfolyós állapotban történik. Szobahőmérsékleten 6 bar nyomáson cseppfolyós halmazállapotú, de hőtágulása jelentős, ezért a tárolótartályok bruttó térfogatának hozzávetőlegesen 80%-át használjuk ki. A tárolási nyomás ingadozása adott, állandó térfogaton, a környezeti hőmérséklet függvényében: -10°C-on 2 bar és +60°C-on 18 bar. Ez szerencsére nem okoz problémát, de a járműbe szerelt tartályt 10 év után nyomáspróbáztatni kell, majd a rákövetkező 5 év után cserélni. Ez a 15 év számos esetben egy személygépkocsi rendszerbentartási időtartamának felel meg. Az eszköz rendszerben-tartásában viszont problémát okoz a járművek hatósági műszaki vizsgáztatása. Időszakos műszaki vizsgát csak a megfelelő engedélyekkel rendelkező vizsgaállomás végezhet, illetve a vizsgát megelőző 30 napon belül egy üzembiztonsági bevizsgálást kell elvégeztetni, melynek a tanúsítványát a műszaki vizsgán be kell mutatni. Ezeket a nehézségeket gondos tervezéssel át lehet hidalni. Az LPG egy korszerű befecskendező-rendszerrel alkalmazva a Magyar Honvédségben rendszeresített személygépkocsi típusok többségében[5] kezelői szempontból nem jelentene komoly problémát. A gépjármű műszerfalán egyetlen kapcsoló lesz a különbség.

3. KÖRNYEZETVÉDELEM ÉS ALKALMAZÁS

A benzin és LPG összehasonlításában, sok tekintetben az utóbbi rendelkezik előnyösebb tulajdonságokkal:

- jobban meghatározható összetevők, közel állandó összetételi aránnyal, míg a benzin mintegy 400 féle összetevőt tartalmaz[6];

[4] A propánbutánt 40% C_3H_8 – propán és 60% C_4H_{10} –bután alkotja. Az szabvány által előírt tüzelőanyag maximum 5%-a lehet valamilyen nehezebb szénhidrogén. Oktánszáma a 95-ös benzinével megegyező, illetve annál magasabb. [10]

[5] Skoda Octavia 1.6 l-es AEE; VW Bora AEH, BFQ motor, Opel Astra 1,4 és 1,6 l-es C14NZ, C16NZ illetve ezek korszerűbb továbbfejlesztett motorokkal szerelt változata.

[6] A benzin minőségét meghatározza: MSZ EN 228:2009, illetve a mindenkori szabvány [11]

- magasabb kopogástűrés, korszerű motorvezérlési rendszereknél jobban optimalizálható égésfolyamatokat eredményez (bár a teljesítmény valamelyest csökken, a motor forgatónyomatéka alacsony, és közepes fordulatszámán növekszik);
- a gyújtógyertyák, és a motorolaj igénybevételei csökkennek, ezzel élettartamuk megnő (a gyújtógyertyák kevésbé szennyeződnek, ezzel javulnak a hidegindítási tulajdonságok);
- LPG üzem esetén nincs szükség tüzelőanyag tápszivattyú működtetésre, ezzel az alkatrész élettartama növekszik, csökken az eredeti tüzelőanyag-ellátó rendszer meghibásodásának lehetősége;
- a keverékképzés során sem szilárd, sem folyékony halmazállapotú tüzelőanyag nem kerül az égéstérbe, ez által nincs koromképződés[7] a kipufogórendszerben;
- sem az összetevők, sem az égéstermékek nem mérgezőek (oxigén-kiszorító hatásúak);
- az üzemeltetés az LPG árának köszönhetően gazdaságosabb.

4. KARBANTARTÁS ÉS VÁRHATÓ MEGHIBÁSODÁSOK

A haditechnikai eszközök fejlesztése, átalakítása kizárólag olyan kihatással lehet az eszköz alkalmazási körülményeire, amelyet az eszköz karbantartási rendszerének átalakításával ki lehet küszöbölni, figyelembe véve az átalakítás eredményének pozitív hatásait. Egy korszerű benzinüzemű belsőégésű motor tervezésekor alkalmazott biztonsági tényezők lehetővé teszik, hogy az LPG üzem okozta megnövekedett termikus igénybevétel ne okozzon szerkezeti károsodást. Az LPG üzemhez szükséges levegő/tüzelőanyag tömegarány 15,5:1, míg a benzin esetében ugyanez az érték 14,7:1, azaz ugyanakkora hengertérfogatra mérsékeltebb tömegű LPG jut be szívás ütemben, mint benzinből. Az LPG égési hőmérséklete mintegy 150°C-kal magasabb a benzin 2000°C–os égési hőmérsékleténél, de a kisebb tömegű elégett szénhidrogén ezt valamelyest kompenzálja. A helytelen beállítás eredménye lehet a szegénykeverékes üzem, mely rendkívüli mértékű termikus terhelést jelent a motornak az égés idejének elhúzódása miatt.

Felmerül még a szelepek kenésének az úgynevezett felsőkenésnek az igénye. Gyakorlatilag ugyanúgy, mint egy dízel üzemű motor esetében itt sincs kenése a szelepeknek, a szelepvezetőknek, illetve a szelepülékeknek. [3] A korszerű benzinmotorok mintegy 95%-a nem igényel ilyen kenést, ezt azzal indokolhatjuk, hogy a gyártók tudatosan csökkentik az általuk gyártott járművek érzékenységét a helyi kereskedelemben kapható tüzelőanyag minőségére, esetleg azok szegényes adalékolására.

5. ALKALMAZÁS FELTÉTELEI A MAGYAR HONVÉDSÉGBEN

Fontos kérdés, hogy egy LPG rendszer beépítése után milyen módon lehet megoldani a tüzelőanyag-felhasználás dokumentálását, okmányolását.

A Magyar Honvédség gépjármű-technikai eszközeinek igénybevétele a besorolásuk alapján történik. A besorolási parancs tartalmazza többek között az eszköz éves kilométer és üzemanyag kiszabatát [5] [6]. Ennél az okmánynál már szükséges egy olyan módosítás, amely lehetővé teszi az eszközök két tüzelőanyaggal történő üzemeltetését.

A Magyar Honvédség nem rendelkezik LPG tankolására, tárolására és szállítására alkalmas eszközökkel, így mindenképpen csak külső forrásból lehet megoldani ezt a

[7] Az Euro 3-as környezetvédelmi besorolású benzinmotoroknál jellemzően megtalálható a kipufogógáz visszavezető rendszer. E rendszernek egyik fontos eleme az EGR szelep, melynek meghibásodását a koromképződés okozza.

problémát. Ez szintén megoldható, amennyiben az üzemanyagtöltő állomással nem rendelkező honvédségi szervezetek mintájára üzemanyagkártyával vásárolnak tüzelőanyagot. Szolgálati, parancsnoki, illetve futár célokat szolgáló járműpark benzinüzemű állományát érinti elsősorban az átalakítás lehetősége.

További problémát jelent, hogy meg kell határozni az üzemanyag fogyasztási normát az alternatív tüzelőanyagra. A legcélszerűbb forrás ez esetben az LPG rendszer forgalmazója. Ez várhatóan a benzinre megállapított norma 120% körüli értéke, azaz 8 literes norma esetén 9,6 liter 100 km-re. Az igénybevétel megkezdésekor a motort benzinnel kell elindítani. Egészen addig benzin a felhasznált tüzelőanyag, amíg a hűtőfolyadék hőmérséklete el nem éri a 35-40°C hőmérsékletet. Az előre meghatározott hőmérséklet elérése után gázelvételre, vagy gázadásra történik a tüzelőanyag rendszer álkapcsolása. Ebből adódik, hogy a benzinfelhasználást is regisztrálni kell. Egy jól beállított LPG rendszer átkapcsolása a legtöbb esetben még a telephelyen megtörténik az eszköz 1-es számú technikai kiszolgálásának elvégzése közben, esetleg rövid idővel később.

Meg kell határozni a fogyasztás okmányolásának menetét, módját. A Magyar Honvédség haditechnikai eszközeinek tüzelőanyag-felhasználását a legfontosabb menetokmányon, a menetlevélen, illetve az üzemóralapon rögzítik. Az átalakításra alkalmas eszközök igénybevételét menetlevél alapján kezdheti meg a kezelőszemélyzet, ezért az üzemóralappal ez a cikk nem foglalkozik.

A legcélszerűbb egy kiegészítő okmány megszerkesztése, amit a menetlevélhez kell csatolni. Ezen az okmányon kell feltüntetni az LPG tankolásának helyét, időpontját, a tankolt mennyiséget, a kilométeróra pontos állását. Az okmány a menetlevéllel együtt kerül leadásra, illetve feldolgozásra. A kedvezményes térítéses, illetve a térítéses igénybevétel esetén az igénybevett eszközt a laktanyához legközelebb eső üzemanyagkúton meg kell tankolni, illetve a tankolás tényét dokumentáló számlát a menetlevélhez kell csatolni. Ez egy jól bevált, működő rendszer, melynek mozzanatait mintául véve lehetőség nyílhat az LPG felhasználás rendszerének kidolgozására.

Egy átalakított gépjárműben valamelyest lecsökken a csomagtartó hasznos térfogata is. Amennyiben úgynevezett pótkeréktartályt alkalmaznak, a pótkerék kerül a csomagtartóba. Ez, azoknál az eszközöknél, amelyek a vizsgált csoportba tartoznak, nem fontos szempont[8].

6. AZ LPG ALKALMAZÁSÁNAK ELŐNYEI

Mindenképpen számításba kell venni a felmerülő, illetve a megtakarítható költségeket. Számtalan magyarországi vállalkozás foglalkozik gázautó átalakítással. Egy nagy darabszámú flotta átalakítása az átlagos piaci árnál jóval előnyösebb lehetőségeket jelent. Egy hétköznapi gépkocsi korszerű szekvenciális rendszerrel [9] való ellátása, 300 000 HUF alatt van. Ez tartalmazza a Környezetvédelmi felülvizsgálat, és a kettős üzem forgalmi engedélybe való bejegyzését is. Egy honvédségi személygépkocsi tervezett kilométer kiszabata 300 000 km. Amennyiben ezt évi 20 000 kilométer futás-teljesítménnyel teszi meg 15 év alatt, úgy évi egy ellenőrzés és szűrőcsere lesz esedékes. A 15 évre tervezett rendszerbentartás alatt 6 műszaki vizsga, és az ezzel járó gázbiztonsági felülvizsgálat, és egy nyomáspróba költségét kell előre tervezni. A benzin felhasználása az eszköz indítása után mindkét tüzelőanyag fajta használatakor jelen van, így azt 10%-ra megállapítva (30 000 km) külön tételként kell kezelni.

[8] A Magyar Honvédségben speciális esetben szükség lehet ezen eszközök csomagtartó kapacitására, pl Baleseti helyszínelő gépkocsi esetében. A pótkerék nem foglal számottevő helyet.

270 000 km alatt felhasznált LPG ára	2700 x 9,6 x 230 =	5961600
270 000 km alatt felhasznált benzin ára	2700 x 8,0 x 420 =	9072000
30 000 km alatt felhasznált benzin ára	300 x 8,0 x 420 =	1008000
300 000 km alatt megtakarított költség		3110400

egyszeri beépítési összeg	1 x 300000 =	300000
20000 km-ként átvizsgálás 15 alkalommal	15 x 10000 =	150000
Műszaki vizsga, és a gázbiztonsági tanúsítvány díja (15 év alatt 6 alkalom)	6 x 25000 =	150000
Tartály nyomáspróba (1 alkalom, a 10. évben)	1 x 15000 =	15000
Költségek összesen		615000

1. táblázat. Gazdasági kalkuláció forintban (HUF)

A kalkuláció alapján a mai műszaki vizsga költségekkel és üzemanyagárakkal számolva 2 500 000, azaz kétmillió-ötszázezer forint takarítható meg járművenként. A teljes futásteljesítmény 10%-át csak szélsőséges esetben futja egy LPG–re átalakított személygépkocsi benzinnel, ez az érték valójában 2-3% között kalkulálható. Amennyiben az eszköz túlüzemeltetésére kerül sor, abban az esetben a 15 év elteltével további költségek merülnek fel. Az LPG tartályt ennyi idő után cserélni kell, de amennyiben időben előre látható a túlüzemeltetés lehetősége, akkor a nyomáspróba helyett a tartály cseréjét kell végrehajtani. Természetesen a haditechnikai eszközök üzem- és ezen belül tüzelőanyagainak ellátása, annak bekerülési költsége 10 évre előre nem prognosztizálható, de az elmúlt évek civil felhasználása jó kiindulási alap lehet. Előfordulhatnak az LPG rendszert érintő meghibásodások, de a kalkulált megtakarítható összeghez képest ezek elenyésző költséget jelentenek, illetve az első két évben a beszerelést követően garancia vonatkozik a rendszerre.

Az elmúlt tíz évben erősen lecsökkent a személygépkocsik beszerzése a Magyar Honvédségben, ami előrevetíti a jelen eszközpark cseréjét a közeljövőben. Mindenképpen megfontolandó egy megfelelő alkalmazási rendszert kidolgozni, ilyen megtakarítási lehetőség kiaknázására.

Felhasznált irodalom

[1] Nemzeti Tankönyvkiadó Budapest – dr. Dezsényi György – dr. Emődi István – dr. Finichiu Liviu – Belsőégésű Motorok tervezése és vizsgálata

[2] Műszaki könyvkiadó - Bohner-Gschleide-Leyer-Pishler-Saier-Schmidt-Siegmayer-Zwickel: Gépjárműszerkezetek.

[3] Szaktudás Kiadó Ház - Dr. Vas Attila - Belsőégésű motorok szerkezete és működése

[4] Dr. Lakatos István Ph.D. egyetemi docens - Korszerű motordiagnosztika - Alapvető elméleti és gyakorlati ismeretek (2.)

[5] Zrínyi Miklós Nemzetvédelmi Egyetem - Szakmai szabályzatismeret 2001

[6] MH PC És GJMŰ Szolgálatfőnökség - Kézikönyv a páncélos és gépjárműtechnikai szakfeladatok végzéséhez 1996

[7] Gjmű/127 Gépjármű szolgálati Utasítás

[8] 77/2009 (HK 19.) HM FLÜ intézkedés „A Magyar Honvédségben alkalmazott üzemanyagok”

[9] http://www.landirenzo.hu/termekek/lpg; (2012. 02. 10.)

[10] http://www.mol.hu/hu/vallalati_ugyfeleknek/termekek/uzemanyagok/autogaz/; (2012. 02. 10.)

[11] http://www.mol.hu/hu/vallalati_ugyfeleknek/termekek/uzemanyagok/motorbenzin; (2012. 02. 10.)

[12] http://totalcar.hu/magazin/technika/hummerlpg; (2012. 02. 05.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Antal Örs
antal.ors@gmail.com

AZ ÁLLATI TÉNYEZŐ A KATASZTRÓFAVÉDELMI ELŐREJELZÉSBEN

Absztrakt

A katasztrófák elleni hatékony védekezés, valamint a pusztító hatások csökkentése elsősorban a katasztrófák megfelelő előrejelzésével lenne elérhető, azonban a XXI. század tudományosan és technikailag előrehaladott szintje ellenére az eddigi törekvések összességében kudarcot vallottak. Van azonban egy tényező, az állatvilág, ami a mai napig ellentmondásos körülmények között megérzi a földrengések, vulkánkitörések, szökőárak, lavinák vagy akár árvizek közeledtét, aminek magyarázatára a tudomány még nem tudott pontos választ adni. A tanulmány, számos olyan katasztrófa esetet megvizsgálva, amikor az állati viselkedés megfelelő tanulmányozásával és figyelemmel követésével, akár áldozatok százezrei lehettek volna megmenthetőek, bemutatja a jelenséget kutatók eddigi mérföldkőnek számító álláspontjait, és foglalkozik azzal a kérdéskörrel, hogy az „állati jósokon" alapulva, a jövőben növelhető lenne-e jelentős mértékben az előrejelzések hatékonysága.

The efficient defence against disasters and the reduction of the devastating effects could be accomplished by the appropriate forecast of the disasters, although inspire of the technically highly developed level of the 21st century, the current efforts have been failed. Although a very exciting factor exists, which is called zoology, who can sense the danger of earthquakes, volcano eruptions, tsunamis, avalanches or floods in a controversial way. The researchers haven't been able to explain this phenomena, yet. This study introduces the most important points of views of the phenomena by examining numerous disaster incidents, when hundreds of thousands of people could be saved with the appropriate observation of unusual animal behaviours. On the other hand, it concerns about the possibility of a complex disaster forecast system based on animal behaviours in the future, which could highly increase the efficiency of the forecasts.

Kulcsszavak: *magatartásformák, földrengés, evakuáció, kutatás, elektromágneses tér ~ forms of behaviour, earthquake, evacuation, researches, electromagnetic field*

1. BEVEZETÉS

A állatok katasztrófákat megelőző viselkedése tanulmányozásának egyik leghíresebb kutatója, Helmut Tributsch német fiziko-kémikus professzor is alátámasztja azt az állítást, miszerint a napjaink legpusztítóbb természeti csapásának számító földrengésekre utaló jeleket az atmoszférában bekövetkező változások idézik elő. Három fő jelenség ismert; az intenzív felhő- és ködképződés, az atmoszférában megjelenő szokatlan fényjelenség és az állatvilág szokatlan viselkedése. *[1]*

Ez utóbbi témával részletesen foglalkozva, a tanulmány során az olvasó komplex betekintést nyerhet az állatvilág mai napig vitatott és ellentmondásokkal teli reakcióira olyan természeti katasztrófákat megelőzően, mint az említett földrengések, a szökőárak, az árvizek, a lavinák vagy akár a vulkánkitörések. Az emberi tényező, azaz a technikai eszközök igen magas fejlettsége ellenére az előrejelzési statisztikák rendkívül alacsony hatékonyságot mutatnak, szemben az állatvilággal, amely egyértelmű jelekkel képes kifejezni, hogy veszélyhelyzet közeleg. Mivel az állatvilágra jellemző, hogy összhangban élnek, tömegesen tudnak azonnal reagálni a veszélyre, amit kényszeres meneküléssel fejeznek ki. Felmerül a kérdés tehát, hogy van-e lehetőség az állatok viselkedésén alapuló előrejelzési illetve megelőzési rendszer kialakítására, amely jelentősen hozzájárulhatna a természeti katasztrófák áldozatai számának csökkentéséhez. A tudósok a témával kapcsolatos állításaikat a mai napig inkább csak kísérletekre és találgatásokra alapozzák, sok esetben egymásnak ellentmondó megállapításokkal, melyek szorosan összefüggnek az egyes fajok úgynevezett „hatodik érzékének" lehetőségével, illetve azzal a kérdéskörrel, hogy melyek azok a katasztrófahelyzetből fakadó folyamatok amik az állatokban különleges biológiai reakciókat váltanak ki.

Témaválasztásomban jelentős szerepet játszott a természeti katasztrófák iránti érdeklődés, illetve azok folyamatos bekövetkezése illetve aktualitása, valamint az a feltételezésem, hogy az állati ösztönöket tudományosan alábecsülik annak ellenére, hogy a kutatások kiterjesztésével hosszú távon milliók lehetnének megmenthetőek.

A téma kifejtése során jól tudtam támaszkodni a Gerold Hofmann által rendezett „Sense of Danger" című dokumentumfilmre [1], amely kiválóan foglalta össze az egyes szakértők és tudósok hipotéziseit az elemi csapásokat megelőző szokatlan állati magatartásformákról, továbbá kutattam a szokatlan viselkedéseket kiváltó fizikai jelenségeket és állati adottságokat, látni fogjuk azonban, hogy a tudomány az út elején jár még a témát illetően.

2. AZ ÁLLATVILÁG VISELKEDÉSE A TERMÉSZETI CSAPÁSOKAT MEGELŐZŐEN

A vadon élő állatok és a házi kedvencek természeti csapásokat megelőző furcsa viselkedésének ismerete nem új keletű dolog. [2] Korábbi feljegyzések tanulmányozásakor egészen az i.e. 373-ig mehetünk vissza, amikor írásban rögzítették az állatok (főként kisméretű hüllők, kétéltűek és rágcsálók) gyors menekülését pusztító földrengést megelőzően. A későbbi évszázadok során egészen napjainkig szinte megszámlálhatatlan feljegyzést és esetet említhetünk meg szokatlan állati viselkedésekről, azonban komoly kutatómunka csak az elmúlt évtizedben irányult a jelenség kérdéseinek megválaszolására. A továbbiakban a katasztrófát megelőző furcsa viselkedési formák tárgyalására kerül sor.

2.1. A csapásra utaló jelek

Az állatok szokatlan viselkedése fajonként különbözhet természetesen a sajátos adottságaiknak és adaptációiknak köszönhetően. A közös reakció a menekülési kényszerben, a „menekülési ösztön" megnyilvánulásában jelenik meg. Egyes fajok, például a majmok vagy

kisebb rágcsálók (mókusok, patkányok, egerek stb.) viselkedésén megfigyelhető, hogy pánikszerűen magaslati pontokat keresnek, mint a villanypóznák, háztetők vagy oszlopok a szökőár-csapást megelőzően. Számos esetben megfigyelhető volt a kígyók vagy földigiliszták tömeges megjelenése a földfelszínen, téli hónapokban olykor a fagyhalálba menekültek a talajrétegbeli búvóhelyeikről. Ugyancsak szokatlan esemény a városok utcáit ellepő varangy vagy béka invázió (1. ábra), ami szintén közelgő természeti csapásra utal.

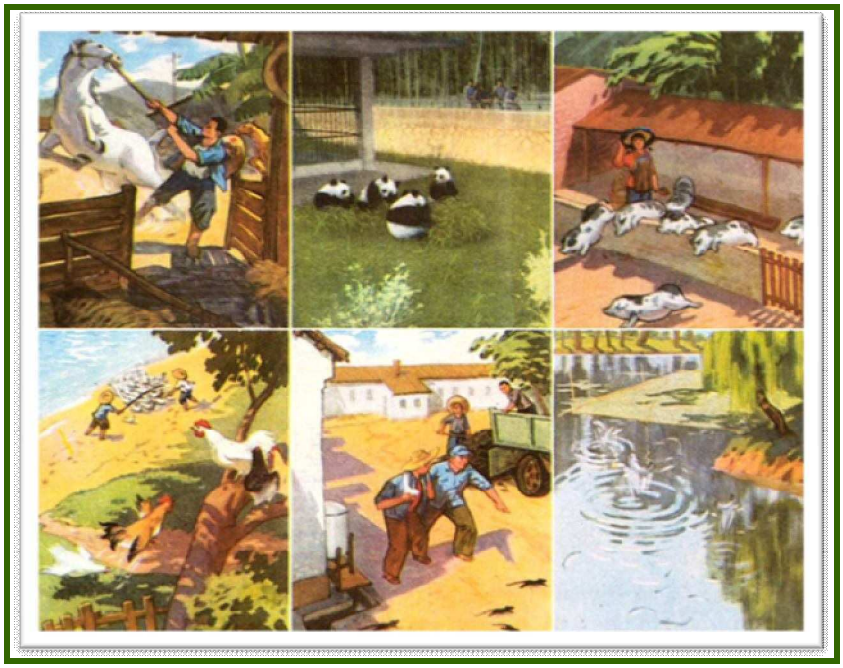
1. ábra. Békainvázió Kínában két nappal a földrengés előtt
Forrás: http://www.pinewooddesign.co.uk/2008/05/12/earthquake-cloud-prediction/; (2012. 02. 19.)

Szinte minden vadon élő emlősnél megfigyelhető a veszélyeztetett terület minél gyorsabban való elhagyása, általában már napokkal a katasztrófa bekövetkezése előtt. Ilyenkor általában tömegesen húzódnak be az erdőkbe, vagy magaslati menedékhelyeket keresnek a veszélyzónától távolabb eső hegyeken. A szokatlan viselkedés természetesen a vízi élővilágra és a madarakra is megállapítható.

Katasztrófa-sújtotta területeken élő halászok megfigyelései alapján elmondható, hogy a partvidéken gyakori halfajok hirtelen eltűnése, valamint más mélytengeri élőlények felszínen folytatott szokatlan aktivitása előzte meg számos esetben a katasztrófákat. A menekülési ösztön egyik kísérő jelenségére gyakori példa az állatok hangos és nem megszokott zajongása és „kommunikációja", ami elsősorban a madarakra jellemző, de ugyancsak a nyílt tengeren halászók elmondása alapján - az állatvilágban kimagasló intelligenciával rendelkező - delfinek jelezték nekik a veszély közeledtét azzal, hogy csónakjuknál hangokkal adtak jelzéseket nekik, és orrukkal a csónakok oldalát csapkodták, ami teljesen szokatlan tőlük. [3]

A vadon élő állatok mellett a háziállatok is képesek érzékelni a katasztrófa veszélyeket, és a szabadban élő társaikhoz hasonlóan szokatlan reakciókat váltanak ki bennük, legtöbb esetben a bezártság az, ami korlátot szab menekülésüknek. A kutyákra elmondható, hogy nagyon nyugtalanná és agresszívé vállnak, hangosan ugatnak és vonyítanak, emellett fontos megemlíteni, hogy a földrengéseket megelőzően drasztikusan megnő az elszökött kutyák száma, amiről a későbbiekben még szó esik. A kalitkába és ketrecbe zárt madarak és rágcsálók pánikszerűen próbálnak kijutni „fogságukból", a díszhalaknál is megfigyelhető, hogy felgyorsulva fel-alá úszkálnak az akváriumokban. Több földrengés után érkeztek olyan beszámolók, amelyek szerint a csapást megelőzően a méhkaptárokból hirtelen eltűntek a méhek, a farmokon pedig teljes volt a felfordulás a különböző takarmányállatok pánikszerű viselkedése miatt. Ugyanez elmondható az állatkertekre is ahol olykor kaotikus állapotok

uralkodik el, egyértelmű jelet adva, hogy valami nincs rendben. A következő ábra (2. ábra) néhány jellegzetes állati magatartásformát illusztrál, amik gyakran tapasztalhatóak földrengések, vulkánkitörések, vagy szökőárakat megelőzően.



2. ábra. Természeti csapásra utaló állati magatartásformák,
Forrás: Magyarország Földrengési Információs Rendszere

Evidens, hogy minden érintett állatfaj katasztrófát-megelőző viselkedésének tárgyalására nincs mód, azonban összegzésképpen elmondható, hogy a maga módján és adottságin alapulva a nagytestű emlősöktől a rovarokig a denevéreken át, szinte az összes fajra megállapítható, hogy képesek időben reagálni a veszélyhelyzetre.

Alapvetően az ember elsősorban a nagyobb testű gerincesek és emlősök szokatlan viselkedésére lesz figyelmes, azonban a rovaroknál, hüllőknél és kétéltűeknél is olykor inváziószerűen megfigyelhető a „pánik" jelenség, ami a gyors menekülésben, vagy menedékhely keresésében fejeződik ki. A következőkben tárgyalt esetek jól demonstrálják, hogy milyen esetekben fordulhat elő az ember száméra szokatlan állati viselkedésmód katasztrófahelyzeteket megelőzően.

2.2. Konkrét esetek, ahol az állatok egyértelműen figyelmeztettek a veszélyre

„A katasztrófák közül a legösszetettebb pusztító hatással és kárterületekkel a földrengések rendelkeznek. Egy földrengés-sújtotta területen a rengések erősségétől függően, az infrastruktúrák (épületek, közművek, utak, hidak, közlekedési csomópontok stb.) részben vagy teljesen rombolódhatnak." [13] Itt nagyon fontos az időtényező. Az állatok jelzését előbb észlelhetik az emberek, mint a védelmi rendszerek riasztását. Ebben a szakaszban néhány olyan földrengés és egyéb estet, amelyeknél a szakirodalmak megemlítik, hogy az állatok viselkedése figyelmeztetett a veszélyre:

- *San Francisco, 1906, földrengés:* A kaliforniai San Francisco az Észak-amerikai-kőzetlemez és a Csendes-óceáni-kőzetlemez között húzódó Szent András-törésvonal mentén igen aktív szeizmikus zónában terül el, aminek köszönhetően nagyon gyakoriak a földrengések. 1906-ban a megszokottnál jóval nagyobb erejű, a Richter-skála1 szerinti 7,8-as erősségű rengés sújtotta a várost, amely szinte

1Richter-skála: A földrengések energiájának a pontos megállapítására bevezetett skála, mértékegysége a magnitúdó (M) [4]

teljesen elpusztult, több mint 7000 áldozatot követelve. Számos jelentés számol be arról, hogy a csapást megelőző órákban, a háziállatok rendkívül szokatlanul és zavartan viselkedtek, főként a kutyákon és a macskákon volt megfigyelhető. [1]

- *Haicheng (Kína), 1975, földrengés:* A kínaiak, a japánok mellett, már ősidők óta ismerték és tanulmányozták az állatok furcsa viselkedését természeti katasztrófákat megelőzően és a mai napig nagyon komolyan foglalkoznak a kérdéskörrel. 1975-ben a fagyos téli hónapok ellenére a kígyók a felszínre jöttek, a háziállatok és rágcsálók pánikszerűen keresték a magaslatokat, a lovak elszabadultak és a kutyák is látszólag indokolatlanul agresszívvé váltak. Az ősi korszakra visszavezethető ismereteikre és az állatvilág szokatlan viselkedésére alapozva 200.000 embert evakuáltak többek között Haichengből egy nagyon erejű földrengés előtt. Ezt a mai napig az egyetlen olyan esetként tartják számon, amikor az állatok viselkedését figyelembe véve tömeges kitelepítést hajtottak végre. Helmut Tribusch egy egy évvel korábbi, Haichenghez közeli kisebb földrengés előzményeit is feleleveníti „When the Snakes Awake (Amikor a kígyók éberek)" című könyvében; *„a libák felrepültek a fákra, a malacok megtámadták egymást vagy kikaparták a földet az ól kerítése alól…a kerti tóból gázbuborékok jelentek meg"*. [3]
- *Tangshan (Kína), 1976, földrengés:* Az egy évvel korábbi esetből sajnálatos módon nem okulva, 1976-ban Észak-Kínában 250.000 emberéletet követelt egy 7,8-as erősségű2 földrengés. A Haicheng-hez hasonló állati viselkedésből eredő előjelek ellenére nem rendeltek el evakuációt. [1]
- *Kobe (Japán), 1995, földrengés:* 1995 januárjában Richter-skála szerinti 6,9-es erősségű földrengés rázta meg a japán várost több ezer embert romok alá temetve. A túlélők elmondása szerint az állati előrejelzés ismét működött, kitelepítésre azonban ezúttal sem került sor. [6]
- *Paznaun-völgy (Ausztria), 1999, lavina:* Ausztria Tirol tartományában történt az elmúlt évtizedek legsúlyosabb lavina katasztrófája, 170.000 tonna hó zúdult az alpesi Galtür falura. A hótakaró alatt 31 ember lelte halálát. A lavina megindulását megelőző napokban megfigyelhető volt, hogy az alpesi vadjuhok lehúzódtak a völgybe, annak ellenére, hogy a téli hónapokban a magaslati menedékhelyeket keresik magukat. [1]
- *Sri Lanka, 2004, szökőár:* A 2004-es tenger alatti földrengés által kiváltott Indiai-óceáni szökőár következtében a szigetország Sri Lanka partvidékének csaknem kétharmada megsemmisült kb. 45.000 lakos halálát okozva. Ennek ellenére a területen egyetlen szabadon élő emlős állati tetemet nem találtak a szökőárat követően, mivel a veszélyt megérezve időben elmenekültek a partvidékről. [1]
- *Tájföld, 2004, szökőár:* A 2004-es szökőár a tájföldi partvidéken is óriási pusztítást végzett, számos üdülőfalut megsemmisítve az ott tartózkodó helyi lakosokkal és külföldi turistákkal. Helyi halászok és búvárok elmondása szerint egész delfincsapatok jelezték nekik a veszély közeledtét. Egy másik tájföldi településen, Phuket-en, elefántok szabadultak el gazdáiktól illetve egy egész csapat turistával a hátukon menekültek a domboldalra közvetlenül a végzetes árhullám érkezése előtt. [1]
- *Pakisztán, 2005, földrengés:* A 2005-ben a pakisztáni Kasmir tartományban kipattant Richter-skála szerinti 7,6-os erősségű földrengés is több tízezer áldozatot követelt. Ebben az esetben is számos egyértelmű állati jelzést említhetünk meg a madarak hangoskodásától a vadállatok eltűnéséig. [1]

2Magnitúdó: A földrengés epicentrumától számított 100 km-re vonatkoztatott maximális amplitúdójának a 10-es alapú logaritmusa [4]

- *Szecsuán (Nyugat-Kína), 2008, földrengés:* 2008-ban a kínai Szecsuán tartományban ismét nem a kitelepítés mellett döntöttek, ami megint hibás lépésnek bizonyult. A tartománybeli Mianzhu várost békák ezrei lepték el, azonban helyi szakértők ezt normális jelenségként kezelték. Két nap múlva a városban több ezer ember halt meg 7,8-as magnitúdójú földrengés következtében. A veszélyhelyzetet tovább erősítette, hogy a földrengés epicentrumától kb. 1000 km-re, a wuhani állatkertből is rendkívül szokatlan állati viselkedést jelentettek; a zebrák ki akartak törni, az elefántok ormányukkal csapkodtak, és gondozóikat is megtámadták, illetve az állatkert többi lakója is nagyon nyugtalanul viselkedett. [7]
- *L'Aquila (Olaszország), 2009, földrengés:* A l'aquilai intenzív földrengést is érdekes, állatokkal kapcsolatos jelenségek előzték meg. A legfurcsább eseményként kezelik a tudósok azt, hogy a város egyik tavából egyik napról a másikra egy jelentős varangykolónia teljesen eltűnt. [8]
- *Christchurch (Új-Zéland), 2011, földrengés:* Kevesebb, mint 48 órával egy új-zélandi földrengés előtt 107 gömbölyűfejű-delfin vetette magát partra és pusztult el (3. ábra). Az eset lehet akár véletlen egybeesés is, de számos alkalommal számoltak be delfinek és bálnák öngyilkos partra vetődéséről földrengést vagy szökőárat megelőzően. [9]

3. ábra. Öngyilkos cetek Új-Zéland partjainál földrengést megelőzően
Forrás: http://www.guardian.co.uk/world/2011/feb/21/stranded-whales-die-new-zealand; (2012. 02. 20.)

A regisztrált esetek, valamint az elmondások alapján főként földrengések, szökőárak (általában szeizmikus aktivitást követően képződnek) és lavinák esetében volt megfigyelhető az állatvilág katasztrófahelyzetre utaló viselkedése, azonban a tudományos megközelítést és állásfoglalást nem könnyíti meg az esetek különbözősége, valamint az, hogy a különböző fajok nem minden esetben adnak egyértelmű jelzést. Ez ugyancsak alátámasztja a téma további kutatásának szükségességét, keresve, hogy pontosan melyek azok a helyzetek és tényezők, amik befolyásolhatják az állatok szokatlan viselkedését, illetve reakcióidejét. Az említett katasztrófák összehasonlítása során fontos azonosságokat is észlelhetünk, mint a magatartást alapvetően jellemző nyugtalanság, feszültségi inger, és a kényszeres menekülés, valamint az, hogy az állatvilág reakcióban van egymással.

A példának vett esetekből levonható következtetésképpen az is, hogy a katasztrófa bekövetkezését megelőző időben is változó az állatvilág reakciója, ugyanis egyes esetekben napokkal a csapás előtt tapasztalható volt a szokatlan viselkedésmód, de előfordultak olyan esetek is, amikor közvetlenül a katasztrófa előtt 1-2 órával reagáltak csak meneküléssel.

3. AZ ÁLLATOK KÜLÖNLEGES ÉRZÉKELÉSE

A tudóstársadalmat is erőteljesen megosztja az a kérdéskör, hogy melyek azok a katasztrófahelyzeteket megelőző hatások illetve tényezők, amik kiváltják az állatokban a szokatlan viselkedést és az azonnali menekülési kényszert. Általánosságban elfogadott elméletet nem sikerült még alkotni, azonban számos elképzelés látott napvilágot az infrahang-érzékeléstől az állatok hatodik érzékéig, amelyek közül sokat tudományos kísérletekkel sikerült is alátámasztani. A következőkben ezen elgondolások boncolgatása következik, levonva a következtetéseket keresve a legvalószínűbb elméletet illetve elméleteket, amik alapot adhatnak a további kutatások céljából.

3.1. Az infrahangok

Az egyik megalapozottnak vehető elmélet szerint egyes fajok képesek érzékelni a földrengések vagy vulkánkitörések kialakulásából eredő nagyon alacsony frekvenciájú hangokat. Mint ismert, az emberi hallás tartománya 20 Hz-től 20 kHz-ig terjed, az említett hangok pedig bőven a 20 Hz alatti, úgynevezett „infrahang" tartományba esnek, amik érzékeléséhez az állatok érzékszervei adaptálódva vannak. Az infrahang jelekre jellemző, hogy föld, víz és levegő közegben is nagyon gyorsan akár több ezer km-re is terjedhetnek. Sőt, egyes fajok speciális hangképző szervekkel is rendelkeznek, amikkel az infrahang „csatornákon" kommunikálni is tudnak társaikkal, akár figyelmeztetni őket a közelgő veszélyről.

Az infrahangokat ugyan az emberek nem érzékelik, mégis bizonyos biológiai hatásokat vált belőlünk is ki, ami általában szorongás és félelem érzetben valósul meg. Az elméletnek tehát van igazság alapja, sőt minden bizonnyal tényleg érzékelnek az állatok alacsony frekvenciájú hangsávokat, azonban kérdéses hogy a különböző fajok milyen minőségben képesek mindezt használni, és hogy tényleg képesek-e „meghallani" a természeti csapásokat. Egyik másik elmélet szerint a kialakult elektromágneses terek váltják ki azokat a biológiai folyamatokat az állatok szervezetében, amik felelősek a furcsa viselkedésért. [2]

3.2. Elektromágnesesség

San Francisco, Kobe, Tanghsan, Szecsuán; néhány példa azon katasztrófahelyszínek közül, ahol magas elektromágneses sugárzást mértek, illetve erős interferencia volt észlelhető a katasztrófát megelőzően és utána is. Az elektromágneses mezőt kiváltó okaként emlegetik egyes tudósok a hirtelen fellépő nyomáskülönbséget, ami a földkéreg egyik legelterjedtebb ásványának számító kvarckristályokból elektromágneses sugárzást vált ki. A tudomány jelenleg még nem tud biztos magyarázatot adni az elektromágnesesség kialakulására, de egy ugyancsak a kőzetekből kiinduló hipotézist is sikerült kísérletekkel alátámasztani, amely szerint a szeizmikus mozgás következtében a földkéreg kőzeteinek töredezésének, illetve kristályszerkezetük bomlásának terméke elektromos áram, ami a felszínen elektromágneses mezőt generál.

Az elektromágnesesség ionizálja a levegőt, ami az állatokban olyan biológiai folyamatokat vált ki (például adrenalin termelés ugrásszerű növekedése), ami az azonnal menekülésre készteti őket. A kőzetanyagokat vizsgálva, a mélységi magmás kőzetek közül (gránit, diorit és gabbró) (4. ábra) az óceáni lemezkérgek fő alkotójának számító gabbró kristályszerkezetének változásánál mértek jelentős elektromosságot. Egyes fajok, mint a delfinek a vízben is képesek érezni az alacsony frekvenciájú elektromos impulzusokat, amit a medencékben végrehajtott kísérletek megerősítenek. [10]

4. ábra. Mélységi magmás kőzetek; Szerkesztette: a szerző;
Forrás: www.termtud.akg.hu

3.3. Az állatok hatodik érzéke

Egyes vélemények „szembe mentek" a tudománnyal, és sok különös, szinte megmagyarázhatatlan, állatvilággal kapcsolatos eseményt a hatodik érzékkel magyaráznak. Köztudott, hogy az ember öt érzékeléssel rendelkezik: a látással, hallással, szaglással, ízleléssel és a tapintással. Mindezek mellett, a feltételezés szerint, az állatvilág rendelkezik olyan hatodik, vagy hetedik érzékeléssel, amivel kapcsolatban az emberi tudomány sötétben „tapogatózik".

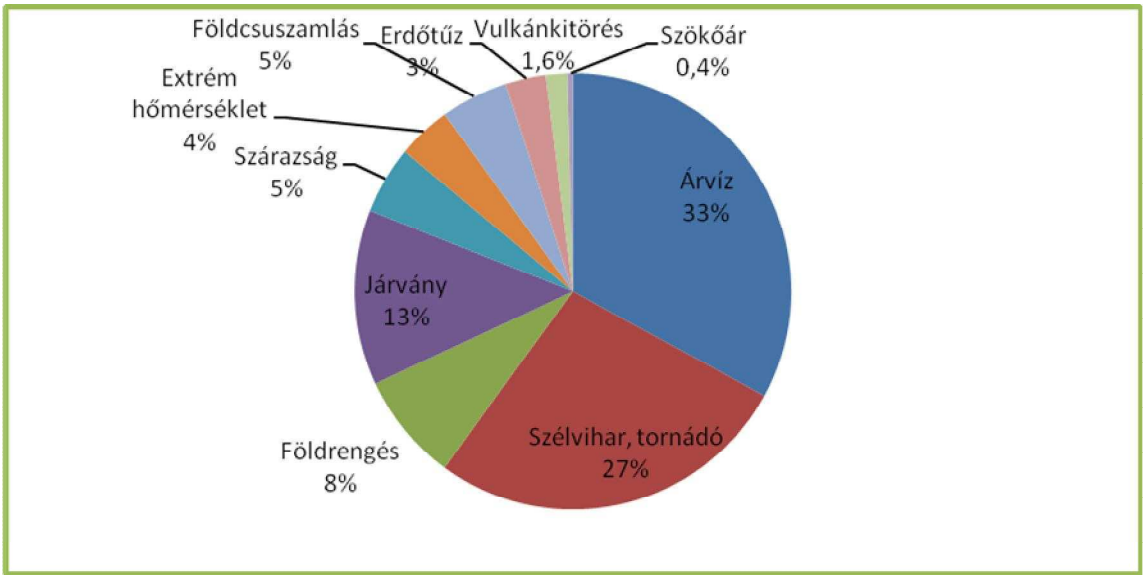
Az állatok kifinomult érzékszerveinek ismerete és további tanulmányozása minden bizonnyal felülírja a hatodik és hetedik érzékükről vélt elképzeléseket, ami által egyes vélemények szerint megérzik előre a halált, a gazdájuk hazaérkezését, a veszélyt, vagy a katasztrófákat is.

Egy interjúban, Kelin Wang geofizikus is tudományos okokkal magyarázza az állatok furcsa viselkedését; *„az állatok nem rendelkeznek hatodik érzékkel, biztosra vehető, hogy geofizikai jeleket érzékelnek"*. [1] Mégis elgondolkodtató az, hogy hogyan képes az állatvilág arra, hogy egy több tízezer emberéletet követelő, egész nemzeti parkot elárasztó szökőár után (Sri Lanka, 2004) egyetlen vadállat tetemére sem bukkannak a mentő alakulatok.

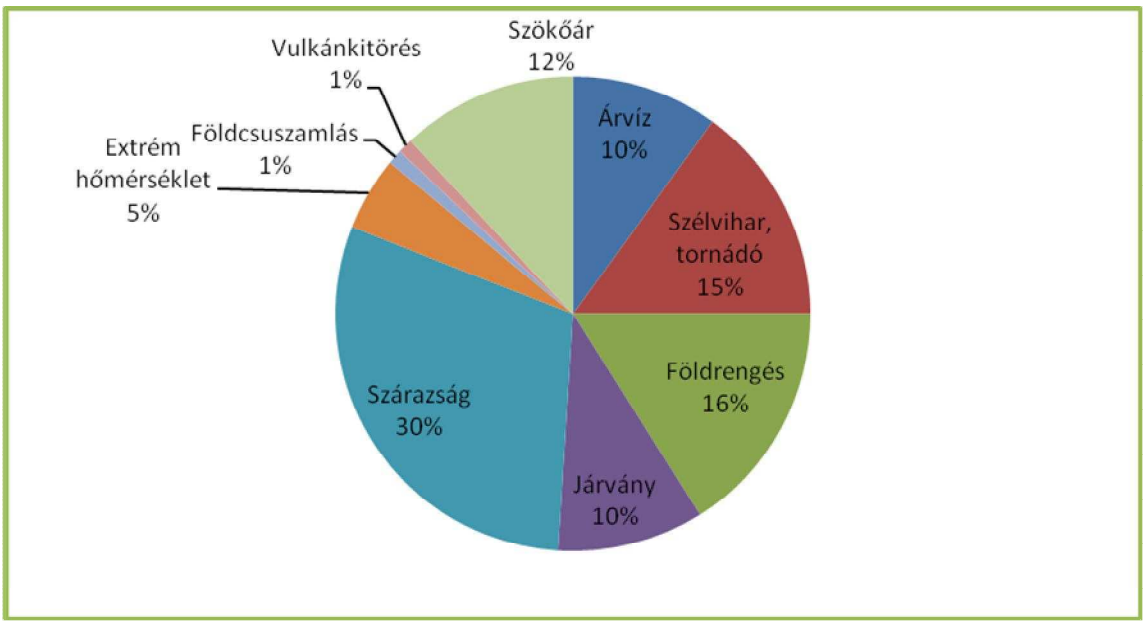
3. AZ ÁLLATI TÉNYEZŐ AZ ELŐREJELZÉSBEN

Ha szemügyre vesszük az elmúlt évtizedekben előfordult katasztrófák eloszlását [5. ábra], akkor megállapíthatjuk, hogy az előforduló jelenségek mindegyikére képes az állatvilág valamilyen módon védekezésképpen reagálni, sőt számos katasztrófa típusra megállapíthatóak az egyes fajok előzetesen vizsgált előrejelzési magatartásformái. Az állati tényező szerepét tovább erősíti azon csapások emberi áldozatainak magas aránya [6. ábra], amikre számos esetben utalnak szokatlan viselkedésükkel.

Az említett adatok is alátámasztják az állati érzékelések és viselkedések kutatásának szükségességét, mivel amellett, hogy sok velük kapcsolatos kérdés maradt még megválaszolatlanul, akár emberek millióinak az élete lehetne megmenthető egy állati viselkedéseken alapuló, hatékony katasztrófavédelmi rendszerrel. Ehhez azonban a kutatások kiterjesztése szükséges felhasználva azon ismereteket, amik az eddigi feljegyzésekből és elmondásokból megállapítható volt. A szkeptikusok táborát erősíti az a tény, hogy a kérdéskör több oldalról való megközelítést igényel.



5. ábra. Katasztrófák eloszlása; Szerkesztette: a szerző; Forrás: http://www.wmo.int/pages/prog/drr/images/pieCharts.png;



***6*. ábra.** Halálos áldozatok száma; Szerkesztette: a szerző; Forrás: http://www.wmo.int/pages/prog/drr/images/pieCharts.png;

Egyrészt nagyon fontos lenne az egyes fajok reakcióinak pontos ismerete, másrészt egyértelműen meg kell határozni, hogy melyek azok a katasztrófahelyzeteket megelőző, fizikai vagy kémiai hatások, amik az állatvilágból kiváltják a szokatlan magatartásformákat és milyen külső tényezőktől függ mindez. Ezen hatások felkutatásában nagy valószínűséggel elmondható, hogy a kőzetlemezek által kibocsátott elektromos impulzusok és az alacsony frekvenciájú hangok vizsgálatával jó úton halad a tudomány, illetve a jelenséget kutató szakértők többsége is egyetért abban, hogy az állatoknak nincs hatodik érzékük, hanem geofizikai jeleket képesek érzékelni.

A kaliforniai James Berkland geológus módszere úttörőnek bizonyult az állatokkal való előrejelzés szempontjából. Köztudott, hogy a Szent András-törésvonal miatt sok kaliforniai település szeizmikusan erősen aktívnak mondható. Berkland az elveszett kutyák és macskák apróhirdetéseit böngészve a helyi lapokban megfigyelte, hogy az előforduló földrengések előtt

az eltűnt házi kedvencek száma drasztikusan megugrik. Elmondása szerint szembemenve a tudományos nézetekkel, ezzel a módszerrel közel 40 éve tudja megjósolni nagy pontossággal a bekövetkező földrengéseket.

Erre bizonyítékul szolgál, hogy az 1989-es Kaliforniában megrendezett baseball világkupa idejére is megjósolt egy nagy erejű földrengést. A mérkőzés sorozatot megelőzően a hirdetések alapján megfigyelte, hogy az elveszett kutyák száma majdnem a négyszeresére ugrott. Eközben San Francisco és Santa Cruz partjainál bálnák vetették partra magukat, ami megerősítette abban, hogy napokon belül földrengés következik és értesítette a sajtót. Igaza lett, a világkupát a Richter-skála szerinti 7-es erősségű földmozgás zavarta meg, több mint 5 milliárd dolláros kárt hagyva maga után. [11]

Az állatok tömeges rendellenes viselkedéseit egyértelmű jelzésként lehet azonosítani valamilyen természeti csapás vagy veszélyhelyzet kialakulására és a vizsgált esetek tanulságaiból is levonható a következtetés, hogy hiba volt a jelenséget komolytalanul kezelni. Ez főként igaz azokra a zónákra, ahol a természeti csapások gyakori előfordulásúak, ugyanis minden esetben a hatékony katasztrófa megelőzés és felkészülés alapja a csapások előfordulásának valószínűségének felmérése.

Dr. Halász László (2009), az érintett területen elismert egyetemi tanár megfogalmazása szerint „a földrengés, vulkánkitörés és árvíz kockázatú területek esetén szükséges egy szakértők által készített térkép, amely jelzi a veszélyeztetett helyeket és a veszély típusát és várható hatását.” [12] Az ezen alapul vett megfigyelések szokatlan állati viselkedésekről felgyorsíthatják a jövőben a lakosságvédelmi és kárenyhítési folyamatokat.

A szakértők arra bíztatnak, hogy addig, amíg a tudomány nem kap választ minden, a témával kapcsolatos fontos kérdésre, addig is a veszélyeztetett területeken élők jobban figyeljenek oda a környezetüket meghatározó állatvilágra, vagy háziállataikra és a akár telefonos veszélybejelentő vonalak igénybevételével is hozzájárulhatnak a tragikus következmények elkerüléséhez illetve csökkentéséhez.

ÖSSZEGZÉS

Az egyes természeti katasztrófákat, mint a földrengést, a lavinát vagy a szökőárat megelőző szokatlan állati viselkedések jellegzetességei és körülményei, valamint az elmúlt évtizedek katasztrófahelyzeteiből levonható tanulságok részletes tárgyalása után következésképpen levonható, hogy egyértelműen szoros összefüggés van az állatvilág magatartása és a veszélyhelyzetek kialakulása között.

Ugyan tudományos módszerekkel még nem sikerült ezt teljes mértékben igazolni, emiatt az eddig kutatások és szerzett tapasztalatok eredménye kevésnek bizonyul egy jól működő állati tényezőre épülő előrejelzési rendszer megteremtésére, mégis számtalan esetben élték túl helyi lakosok a katasztrófákat az állati jelzéseket követve, főként Japánban illetve Kínában ahol ősi hagyományként kezelik az állatok furcsa viselkedésének jelentőségét.

Az irány tehát egyértelmű; az eddigi tudást és geofizikai-kémiai-biológiai kísérleteket követve a tanulmányozást folytatni kell, mert van lehetőség a jövőben akár egy komplex katasztrófavédelmi előrejelzési rendszert alapozni az egyes fajok viselkedésére, valamint betekintést nyerni egy olyan „birodalomba”, ahol az állatvilág messze az emberi képességek felett jár.

A téma kifejtésével megállapítható, hogy a lakosságnak és a védelmi szakembereknek az állatok viselkedésének dekódolása sokat segíthet katasztrófák során, mivel olyan, eddig tisztázatlan tudásanyagra tudnak támaszkodni, ami mérföldkőnek számít az egyes természeti katasztrófák előrejelzése terén és a lakosság riasztása kapcsán, ezért fontos lenne a jövőben ezeket az ismereteket közvetíteni feléjük, és beépíteni a tudásukba illetve képzési anyagukba.

Felhasznált irodalom

[1] Sense of Danger dokumentumfilm, EIKON Media GmbH, 2005, Németország, rendezte: Gerold Hofmann, producer: Ulli Pfau

[2] Vitus D. Dröscher: Ahogy az állatok látnak, hallanak és éreznek, Mi micsoda sorozat 2. kötet, Tessloff és Babilon kiadó, Budapest, 2007, ISBN 978-963-9446-88-5

[3] Helmut Tributsch: When the Snakes Awake, Animals and Earthquake Prediction The MIT Press Classics Series, 1984, ISBN 10:0-262-70025-5

[4] Magyar Larousse Enckilopédia III. kötet, Akadémiai Kiadó, Budapest, 1994. 478. o. ISBN: 963-05-6748-2,

[5] Brian Fisher Johnson: Earthquake prediction: Gone and back again, Earth Magazine, http://www.earthmagazine.org/article/earthquake-prediction-gone-and-back-again; (2012. 02. 19.)

[6] Earthquake devastates Kobe, BBC Home: Archív cikk, 1995; http://news.bbc.co.uk/onthisday/hi/dates/stories/january/17/newsid_3375000/3375733.stm; (2012. 02. 20.)

[7] Pinewood Design: Chinese photographer catch prediction 2 days before earthquake occurred, 2008 http://pinewooddesign.co.uk/2008/05/12/earthquake-cloud-prediction/; (2012. 02. 20.)

[8] Victoria Gill: How animals predict earthquakes, BBC Nature News, 2011. 12. 01.: http://www.bbc.co.uk/nature/15945014; (2012. 02. 20.)

[9] The Guardian: Whales die on New Zealand beach, 2011. 02. 21.: http://www.guardian.co.uk/world/2011/feb/21/stranded-whales-die-new-zealand; (2012. 02. 20.)

[10] Neeti Bhargava, V. K. Katiyar, M. L. Sharma, P. Pradhan: Earthwuake Prediciton through Animal Behaviour, Indian Journal of Biomechanics: Special Issue, 2009. Március; http://www.iitr.ac.in/ISB/uploads/File/ISB/pdf/reviewpaperneeti.pdf; (2012. 02. 20.)

[11] Interview with James Berkland, Animals and Earthquakes; http://animalsandearthquakes.com/james%20berkland.htm; (2012. 02. 20.)

[12] Dr. Halász László: Katasztrófa előrejelzés és helyzetértékelés, ZMNE egyetemi jegyzet 11. o., Budapest, 2009, ISBN: 978-973

[13] Dr. Hornyacsek Júlia: A települési védelmi képességek a katasztrófa-kihívások tükrében, a települések katasztrófa-elhárítási feladatai, a végrehajtáshoz szükséges helyi védelmi képesség alapvető területei, azok kialakításának folyamata. "Biztonságunk érdekében" Oktatási- és Tanácsadó Tudományos Egyesület Budapest, 2011. p. 33. ISBN: 978-963-08-2606-8

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Bárdos Zoltán – Muhoray Árpád
bardos.zoltan@katved.gov.hu – arpad.muhoray@katved.gov.hu

A BELVÍZ KIALAKULÁSA ÉS AZ ELLENE VALÓ VÉDEKEZÉS LEHETŐSÉGÉNEK VIZSGÁLATA

Absztrakt

A belvizek kialakulása a síkvidékek jellemző vízkár formája, az ellene való védekezési módok kialakítását „magyar" módszernek is nevezik. A XX. században kialakított belvízrendszerek és belvízöblözetek, a belvizek jelentős részét el tudták vezetni. Az elmúlt évtizedben a rendkívül szélsőséges időjárási helyzetek következtében súlyos belvízi problémák keletkeztek (1999, 2010-2011), melyek jelentős károkat okoztak a nemzeti vagyonban, a védművekben, műtárgyakban, ingatlanokban és a mezőgazdaságban. Írásunkban a belvizek kialakulását befolyásoló tényezőkkel, a belvízrendezés hidrológiai kérdéseivel, valamint a belvíz elleni védekezés jogi szabályozásának kérdéseivel foglalkozunk. A belvíz elleni védekezés vizsgálatán keresztül a védekezés korszerűsítésére, jobbítására is javaslatokat teszünk.

Inland waters are a typical form of water damage on flat country. The preventive protection method has been named as the „Hungarian" method. The inlets and other flood containment systems, that were set up in the 20th Century, managed to cope with a significant amount of water, but due to the extreme weather conditions in the last decade (1999, 2010-2011), serious problems occurred causing a heavy loss to the national wealth as well as the river management works, residential areas and the whole agriculture. Present writing examines the influential factors, the hydrological questions of inland waters system and the legal regulations. Recommendations are given on the modernization of the protection methods by examining the current methods and system.

Kulcsszavak: *belvíz veszélyeztetettség, védekezés, levezetőrendszerek, talajvíz, vízrendezés ~ inland waters vulnerability, protection, drain systems, subsoil water, underground water, water containment*

1. BEVEZETŐ

Magyarország a Kárpát-medence árvízzel, belvízzel és aszállyal nagymértékben veszélyeztetett területén fekszik. Az elmúlt évtizedekben, hazánkban a rendkívül szélsőséges időjárás következtében az ár-és belvizek, valamint a helyi vízkárok jelentős károkat okoztak. Az ország közel 45 000 km^2 nagyságú síkvidéki területének jelentős részén fennáll a belvíz megjelenésének veszélye. Az ilyen mértékű, rendszeresen visszatérő belvíz elöntés nemzetközi összehasonlításban is egyedi problémát jelent. A hidrológiai tudománya a belvízrendezést egyenesen "magyar" szakterületként tartja nyilván.

Magyarország közel 3200 településének belterülete megközelíti a 664 ezer hektárt, ami az ország területének 7%-a. A településeink közül 1000 síkvidéki, 2200 dombvidéki területen helyezkedik el. Természeti adottságainknak megfelelően a vizek kártételeinek lehetősége síkdombvidéken, településeinken és városainkban egyaránt jelen van. Országosan a települések 40 %-a erősen, mintegy 80 %-a valamilyen mértékben veszélyeztetett a vizek kártételeitől.[1] A belvíz jelenség a síkvidéki területeink sajátos jellemzője és nagyjából az ország 45 %-át érinti. A Duna, a Tisza és mellékfolyóik szabályozási, árvíz-mentesítési munkálatait követően főként a síkvidékeken jelentkeztek belvízi problémák. A belvízi veszélyeztetettség meghatározói egyrészt a természeti adottságokban, másrészt az emberi tevékenységben kereshetők. A természeti tényezők közül meghatározó a területhasználat módja, ami külterületen a helytelen mező- és erdőgazdasági művelésben, belterületeken a mély fekvésű területek beépítésében csúcsosodik ki. A településeken belül szólni kell a szennyvízcsatornázás elmaradásáról, ami az un. "talajvízdombok"[1] kialakulásával nagymértékben hozzájárul a belvíz veszélyeztetettség kialakulásához.[2]

A belvízi veszélyeztetettség jellemzésére mérőszám szolgál, amely figyelembe veszi az éghajlati tényezőket, a domborzati adottságokat, valamint a területhasználat módját. Az Alföld belvízrendszerei eltérő veszélyeztetettségének kialakulásában legnagyobb szerepe a talajnak és a talajvíz mélységének van.

A nyolcvanas és kilencvenes évek aszályos éveiben háttérbe szorult a belvízi kutatások jelentősége. A sokéves csapadékeloszlás ciklusosságát ismerve ugyanakkor nem szabad megfeledkezni a csapadékmaximumok újabb, akár éveken keresztül jelentkező előfordulásáról. Az elmúlt évtizedek földhasználatban, a mező- és erdőgazdálkodás területi struktúrájában – a tulajdonviszonyok módosulása miatt – bekövetkezett változások lényegesen módosították az érintett térségek lefolyási és összegyülekezési folyamatait.[3]

Az alábbi cikkben röviden áttekintjük a szakirodalmat, a hazai belvizek kialakulásának hidromorfológiai hátterét, majd a belvizek elleni védekezés jogszabályi alapjaiból kiindulva a védekezési lehetőségeket és azok megvalósítását vizsgáljuk.

2. BELVIZEK KIALAKULÁSA, KELETKEZÉSÉT BEFOLYÁSOLÓ TÉNYEZŐK

A belvíz, mint a mezőgazdaságban, alkalmanként belterületi épületekben valamint a közlekedési hálózatban komoly károkat okozó jelenség a XIX. századi árvízmentesítési-töltésépítési munkálatok nyomán jelent meg. A megépült árvízvédelmi töltések mentesítették az árterületeket a folyók árvizeitől, ugyanakkor megakadályozták az ármentesített területen belül keletkezett, vagy oda bejutott és a folyók felé törekvő vizek szabad lefolyását. Ezen a

[1] A szennyvízelvezetés igénye mindenki számára természetes, de az érdekfelismerés gyakran csak „az én területemet ne érje” látható gondolkodásig jut el. Az ebből adódó, gyakorlatban elterjedt átmeneti megoldások (szakszerűtlen derítők, un. emésztők, felhagyott kutakba vagy felszíni vizekbe történő bevezetése) a talaj, a talajvíz, a tavak és a vízfolyások elszennyeződését, ill. talajvízdombok kialakulását okozzák, ami bár időben jelentős késleltetéssel ugyan, de nagy veszélyt jelent a vízellátáshoz szükséges felszín alatti mélyebb rétegek vízkészletére is.

problémán először a töltésekbe épített zsilipekkel, később szivattyútelepek kialakításával segítettek.

A belvíz kifejezés már a XIX. század közepétől használatos volt, a fogalom tartalma azonban az idők során folyamatosan változott, sőt valójában ma sem létezik egyöntetűen elfogadottnak tekinthető definíciója. A meghatározások egy része szerint pusztán az ártéren keletkező vizek tekinthetőek belvíznek, azaz keletkezésük alapfeltétele az árvédelmi töltések megléte. Egy másik, mára uralkodóvá vált felfogás szerint az ártéren kívüli síkvidéki területen keletkezett vizek is beleértendők a belvíz fogalmába, vagyis a belvízi jelenség tulajdonképpen az árvízvédelmi töltések kiépülése előtt is létezett. A belvíz definíció szerinti összegzése során a meghatározások tartalmilag megegyeznek abban, hogy „a belvíz a sík vidékek időszakos, de meglehetősen tartós és viszonylag nagy területre kiterjedő jelensége, sajátos vízfajtája".[4] A gátak, töltések, egyéb védművek kiépítettsége, állapota meghatározó az egyes területek árvíz-veszélyeztetettségének megítélésében, sérüléseik, vízállóságuk alapvetően befolyásolják az érintett terület lakosságának, anyagi javainak biztonságát- mindez kölcsönhatásban van belvízveszélyesség kialakulásával, minősítésével.

2.1. A belvizet befolyásoló tényezők

A belvizek kialakulását egyrészt természeti, másrészt emberi tényezők befolyásolják. Meghatározó természeti tényezők közé tartoznak: a domborzati, az éghajlati, a talajtani, a sekélyföldtani és hidrológiai tényezők, valamint a természetes növénytakaró.

A vízgyűjtő terület *domborzati* adottságai döntően befolyásolják a belvízképződést. A belvizek leggyakrabban a környezetüknél alacsonyabban fekvő, katlanszerű, lefolyástalan területen gyűlnek össze. A magasabb területeken beszivárogni nem tudó vizek a mély fekvésű területekre folynak.

Az *éghajlati* viszonyokat jellemzően a csapadék mennyiségének eloszlása jellemzi, ennek megfelelően csapadékos és hűvös éghajlat alatt több belvíz képződik, mint meleg száraz területeken. A belvíz keletkezése szempontjából megkülönböztetnek előkészítő és kiváltó csapadékot. Az előkészítő csapadék a talaj nedvességtartalmát növeli, a belvíz akkor alakul ki, amikor a talaj vízbefogadó-képessége kimerül. A másik legfontosabb meteorológiai tényező a hőmérséklet, amely hatással van a csapadék halmazállapotára és a talaj vízbefogadó képességére is.

A *talajtani* tényezők fontossága abban áll, hogy a vízbefogadó és a vízelvezető-képességet befolyásolják. Minél nagyobb a talaj szabad hézagtérfogata, annál több vizet képes befogadni. Fontos tényező az is, hogy a talaj milyen sebességgel képes a vizet a mélyebb rétegeibe vezetni, ha a talaj-vízelnyelő képessége kevesebb, mint a csapadék intenzitása, akkor belvízelöntés jöhet létre.

A *sekélyföldi tényezők* szoros kapcsolatban vannak a talajtani tényezőkkel, mivel a talajok legalsó „C" szintjét tulajdonképpen talajképző kőzet alkotja. A sekélyföldtani adottságok regionális méretekben szabják meg a talajba jutó víz elhelyezkedését és mozgását, esetleges időszakos felszínre törését.

A *hidrológiai tényezők* közül legfontosabb a talajvíz átlagos elhelyezkedése, amit az előzőekben felsorolt tényezők együttesen határoznak meg. A talajvíz szerepe azért lényeges a belvízképződésben, mert közvetlenül a magas talajvíz csökkenti a talaj vízbefogadó-képességét, szélsőséges esetben teljesen meg is szüntetheti a víz befogadását.

A *természetes növénytakaró* annyira átalakult sík vidékeinken, hogy a belvizek keletkezését befolyásoló hatásairól beszélni az emberi tevékenységek között célszerű.

A belvizek kialakulását befolyásoló emberi tényezők: a terület használat módja, a vízrendezési és meliorációs munkák, valamint a vízháztartási viszonyokat megváltoztató egyéb beavatkozások.

A *területhasználat* során sok esetben átalakul a táj természetes növénytakarója, ami a talaj vízbefogadó-képességét jelentősen befolyásolja. A növények közül az erdőnek a legnagyobb a belvízcsökkentő hatása. Az eltérő talajművelési módok jelentős különbséget idéznek elő a talaj vízviszonyaiban

A *vízrendezési és meliorációs* munkák jelentősen befolyásolják a belvizek keletkezésének feltételeit. Belvízi csatornák építésével, tereprendezéssel, talajcsövezéssel, a szivattyúzás eszközeivel elősegíthető a víz összegyülekeztetése, lefolyása.

A tározók, az öntözőcsatornák és minden olyan létesítmény, ahonnan víz juthat az altalajba megváltoztatja *a vízháztartási viszonyokat*. Például a településeken elszikkasztott szennyvizek a talaj nedvességkészletét, növelik megemelik a talajvíz szintjét. [5]

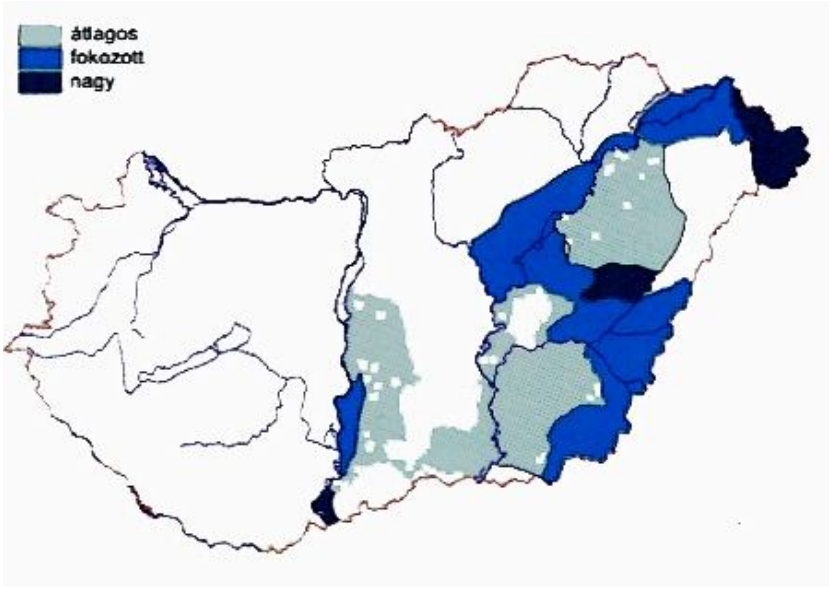
3. BELVÍZ-VESZÉLYEZTETETTSÉGI TÉRKÉPEZÉS

Egy adott térség belvízi veszélyeztetettségét számos természeti és emberi tényező jellemzi, annak térképen való meghatározása elsősorban a tényleges belvízi elöntésekből kiindulva végezhető el megbízhatóan. [1]

Az első, tényleges elöntési térképeken alapuló veszélyeztetettségi térkép az 1970-es évek végén készült, 1:100 000 méretarányban. Az 1980-as évek elején tényleges elöntési felméréseken alapuló, az elöntési gyakoriságot tükröző térképes módszert dolgoztak ki. E belvíz veszélyeztetettségi térképek alapján egy adott terület belvízi veszélyeztetettsége egyetlen mérőszámmal jellemezhető (BV), mely a területek összehasonlítását is szolgálja. [1]

Az utóbbi években a belvíz-veszélyeztetettségi térképezésben is mindinkább teret nyert a korszerű térinformatika, az elmúlt 40 év adatainak számítógépre vitelével egy regionális megbízhatóságú ún. Komplex Belvíz-veszélyeztetettségi Térkép készült el.

Az 1. sz. ábra Magyarország belvíz által veszélyeztetett területeit mutatja, három kategóriát (átlagos, fokozott, ill. nagyfokú veszélyeztetettség) megkülönböztetve.



1. ábra. Magyarország belvíz által veszélyeztetett területei;
Forrás: www.ovf.hu

4. A BELVÍZRENDEZÉS HIDROLÓGIAI ÉS HIDRAULIKAI ALAPJAI

Magyarország kedvező természeti adottságai között a víz szerepének jelentőségét a mezőgazdasági gyakorlat hosszú ideig nem méltányolta. A múlt században megindult

mezőgazdasági fejlődést akadályozta az alföldet időszakosan elborító víz. Amikor elődeink elkezdték az árvíztől mentesített területeken a levezető csatornák létesítését és ezzel a belvízrendszerek kialakítását, akkor új, ezek méretezésével összefüggő problémák jelentkeztek. [5]

A síkvidéki vízrendezés évszázados múltja során számos vízrendezési elmélet alakult ki, azonban négy nagy jellegzetes csoportba lehet őket sorolni:

A *statikus* szemléletű vízrendezési elmélet a vízrendezés kezdeti időszakában keletkezett, amikor a belvíz jelenségét a vízgyűjtő mélyebb részén megjelenő álló víztömegnek tekintették melyet meghatározott időn belül el kell vezetni.

A *dinamikus* szemléletű vízrendezésre a felszíni vízmozgás, a lefolyás és a vizek összegyülekezésének vizsgálata a jellemző, elemei a statikus elemekkel összefonódnak. A vízrendezés hasznosítási kérdéseire azonban az előző elméletek egyike sem tér ki, mindegyik csak levezető vízrendezési jellegű.

A *vízgazdálkodási* szemléletű elméletekben már a csapadék hasznosításával kapcsolatos szempontok is szerepelnek, a talaj mennyi vizet tud hasznosan, illetve kár nélkül tározni és mennyi az elvezethető vízmennyiség.

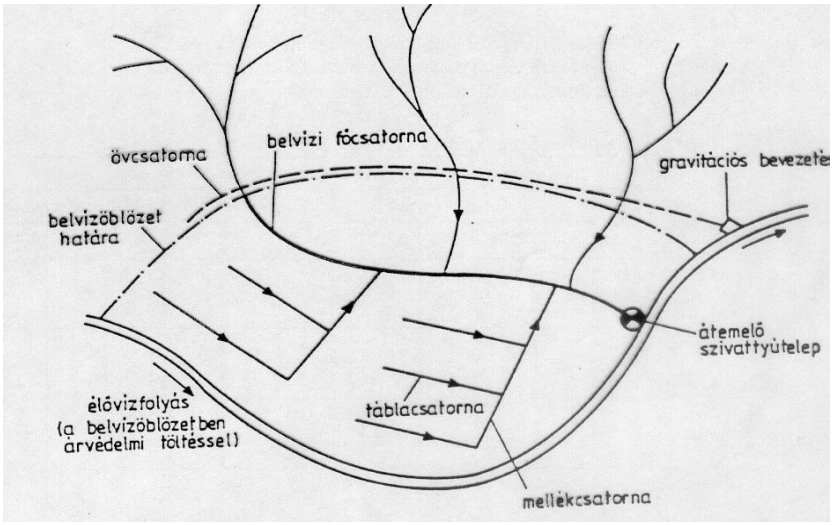
A *rendszerhidrológiai* módszer fizikai-matematikai modelleket alkalmaz, részletesebben tárja fel a síkvidéki, befolyásolt összegyülekezési folyamatokat, és bizonyította, csupán a felszíni vízmozgásra felépített dinamikus elméletekkel nem oldhatók meg a síkvidéki vízrendezés problémái.

5. A BELVÍZRENDEZÉS FELADATAI

A belvízrendszer egy belvízgyűjtő területen tervszerűen létesített belvízgazdálkodási művek összessége, melynek feladata, hogy az egész vízgyűjtőre kiterjedően gazdaságosan oldja meg a belvízlevezetést. A vízrendezés célja, hogy a településeken, ipari területeken a vizeket kártétel nélkül elvezesse, mező-és erdőgazdasági területeken a lehető legjobb kapcsolatot alakítson ki a természetes vizek, a felszíni és a felszín közeli talajrétegek között, nem utolsó sorban pedig a káros vizek elleni védelmet megelőző műszaki megoldásokkal biztosítsa. [6]

A terep esése szerint megkülönböztetünk síkvidéki vízrendezést – más néven belvízrendezést –, valamint hegy és dombvidéki vízrendezést. A vízrendezés területi alapegysége a vízgyűjtőterület, amelynek jellemzője, hogy a felszínen és a felszín alatt összegyülekező vizek egy kilépési ponton hagyják el, illetve vezethetők le dombvidéken vízfolyásokon, síkvidéken belvízcsatornákon keresztül. A kis esésű területeken, a felszínen lefolyó víz sebessége igen csekély, a vízmozgás fékezett, elvezetése nehézségekbe ütközik. Ilyen helyeken a víz természetes körülmények között vissza marad a mélyedésekben és csak mesterséges eszközökkel, létesítményekkel oldható meg az elvezetése. A belvizeket hazánkban 42 400 km hosszú belvízcsatorna vezeti el. Azokat a területeket, amelyekről mesterséges létesítmények vezetik el a vizet, "belvízvédelmi öblözetnek" nevezik. Számuk az országban 85, összes kiterjedésük 43 600 km^2. Kiépítettségük átlagosan a tízévente előforduló belvizek 15 nap alatt történő elvezetését biztosítja. A rendszeren belül a mezőgazdaság számára káros vizeket és a belterületről lefolyó csapadékvizeket nyílt csatornahálózat vezeti le. A levezető hálózat gerincét a főcsatornák alkotják, amelyekre – mint a levélerezet – csatlakoznak a mellékcsatornák, amelyek viszont az alacsonyabb rendű mentesítő csatornák vizeit gyűjtik össze, és továbbítják a főcsatornába. A főcsatorna a belvízrendszer, vagy öblözet összegyűjtött vizeit a főbefogadóba továbbítja, ami általában töltésezett vízfolyás, vagy folyó. A főbefogadóba a vizek gravitációsan, szivattyús átemeléssel vagy a kettő kombinációjával juthatnak el.[6]

A 2. sz. ábra szemlélteti a belvízöblözet felépítését:



2. ábra. A belvízöblözet felépítése
Forrás: www.mgk.u-szeged.hu/download.php?docID=7493

A belvízcsatornák műtárgyai – zsilipek, vízkormányzó műtárgyak – a vízelvezetés szabályozására szolgáló művek. A 3. sz. ábrán egy zsilip látható:

3. ábra. Zsilip
Forrás: www.mgk.u-szeged.hu/download.php?docID=7493

Az utak, vasutak keresztezésében lévő hidak, átereszek a keresztező pályák tartozékai, de a vízátvezetés igényeit is ki kell elégíteniük. A 4. sz. ábrán egy áteresz látható:

4. ábra. Áteresz
Forrás: dunakiliti.network.hu

A szivattyútelepek, szivattyúállások a csatornák vizének befogadóba juttatását biztosítják abban az esetben, ha a gravitációs bevezetés feltételei hiányoznak. Az 5. sz. ábrán egy szivattyú állomás látható:

5. ábra. Szivattyú állomás
Forrás: www.mgk.u-szeged.hu/download.php?docID=7493

A síkvidéki vízrendezési tevékenység nemcsak a belvizek elleni védekezést, a levezetés feladatait foglalja magában. A belvizes és a vízhiányos időszakok váltakozása miatt egyre jobban előtérbe kerül a belvízgazdálkodás. Lényege, hogy a vízrendezési művek célszerű üzemeltetésével a levezetés szabályozható, késleltethető, a belvizek medertározással, övgátolt legelőkön, belvíztározókban visszatarthatók. A belvízgazdálkodás a vízrendezési és a mezőgazdasági tevékenység egységes szemléletű alkalmazásával a belvizes és az aszályos időszakok kártételeinek csökkentésére egyaránt hatékony eszköz.

6. A BELVÍZ ELLENI VÉDEKEZÉS SZABÁLYOZÁSA

Az elmúlt évszázadban hazánkban végzett vízrendezési feladatok, valamint a vízügyi szakemberek munkájának eredményeként a belvíz által veszélyeztetett területeken jól kiépített belvízrendszerek találhatóak. Az elmúlt években-évtizedekben a legtöbb esetben a védművek ellátták funkciójukat és megvédték az emberi életet, épített és természetes környezetet a súlyos károktól. Kedvezőtlen időjárási viszonyok között alkalmanként a belvízi elöntések súlyosabb pusztításokat okoztak, mint az árvizek (pl. 1999., 2010-2011.). A vizek kártételei elleni védekezésre való felkészülés jogszabályi feladatrendszere a Vízgazdálkodásról szóló törvény (Vgtv.), a végrehajtására kiadott 232/1996.(XII.26.) Korm. rendelet (továbbiakban: Kormányrendelet), a 10/1997. (VII. 17.) KHVM rendelet az árvíz- és a belvízvédekezésről (továbbiakban: Miniszteri rendelet), a Vízügyi Igazgatóságok (VIZIG), valamint a vízitársulatok és a települési önkormányzatok felelősségi körébe helyezi a belvíz elleni védekezést. [7] [8] [9]

A Kormányrendelet alapján a védekezésre kötelezettek – a megelőzés érdekében – a felkészülés időszakában kötelesek karbantartani a védműveket, a védekezéshez szükséges gépi, technikai berendezéseket, a különböző felszereléseket, védekezési terveket, különböző nyilvántartásokat készíteni, szükség szerint azokat kiegészíteni, mindezeket évente felülvizsgálni, saját védelmi szervezeteiket megalakítani, azokat felkészíteni, számukra gyakorlatot tartani. E feladatok végrehajtásával végül is egy komplex védelmi felkészülés valósítható meg a belvízveszélynek kitett települések esetében, melynek valóban sarkalatos pontja a vízitársulatok és önkormányzatok által védelmi szakaszonként elkészítendő *Belvízvédekezési terv*, melynek kötelező tartalmi elemeit a Miniszteri rendelet írja elő.

A terv tartalma így kötelezően magába kell, hogy foglalja a:

- védelmi szakasz területének, belvízrendszereinek *műszaki leírását*, - ha a szakasz valamely nagyobb belvízrendszer része, - akkor azon belül a
  - a főcsatornákba torkolló csatornákat a tulajdonosok, egyéb jogcímes használók megnevezésével,
  - a szakasz területén lévő csapadékmérő állomásokat, talajvízszint észlelő kutakat, a vízkormányzás mértékadó vízmércéket, információs hálózatokat,
  - a főcsatornák, szivattyútelepek jellemző adatait,
  - a belvíz tározására igénybe vehető területeket, azok művelési ágait, a tározókat, halastavakat, vízkormányzó műtárgyakat, a szivattyútelepeket, a szivattyú állások üzemelési rendjét, a szállítható szivattyúk tervezett telepítési helyét, kezelőszemélyzetüket, az üzemanyag ellátásukat;
- *áttekintő helyszínrajzot*, amely feltünteti a vízgyűjtő terület határát, a településeket és azok közigazgatási határát, a vízitársulatok határát, a szakasz főcsatornáit, a torkolati szivattyútelepeket, a kijelölt belvíztározókat, a különcélú vezetékes hírközlő hálózatot, az utakat és a vasutakat;
- *részletes helyszínrajzot*, amely az átnézeti helyszínrajzon túlmenően feltünteti a teljes belvízelvezető csatornahálózatot, a szivattyúállásokat, a meliorált területeket, a vízvisszatartásra igénybe vehető területeket;
- *a szakasz és a belvízrendszerek főcsatornáinak hossz-szelvényét és jellemző keresztszelvényeit*, az engedélyezett (tervezett) méretekkel üzemelési vízszinttel és a hozzá tartozó vízhozamokkal, valamint a legutóbbi *állapotfelvételt*, a felmérés időpontjának feltüntetésével;
- a *szivattyútelepek üzemeltetési előírásait*;
- *segédleteket*, korábbi védekezési jelentéseket, felülvizsgálati jegyzőkönyveket, cím- és telefonjegyzékeket;
- a *szakasz védekezési naplóját*.

A szakaszvédelmi terveken túlmenően a VIZIG-ek működési területükre *általános belvíz-védekezési terveket* is készítenek az alábbi kiemelt fontosságú tartalmi részek kidolgozásával:

- a VIZIG síkvidéki területének leírása, a területi egységek lehatárolása, az éghajlati adottságok, a közigazgatási tagozódás, a természetvédelmi területek, a szomszédos államokkal vagy más VIZIG-ekkel összefüggő belvízi művek jellemzői, megállapodásaik, a vízügyi igazgatóság, vízitársulások, önkormányzatok, gazdálkodó szervezetek vagyonkezelésében lévő belvíz-védekezési létesítmények és eszközök jellemzői és átfogó leírása;
- a belvízvédekezés személyi (átlagos létszámszükséglet) és tárgyi feltételei;
- helyszínrajz, a VIZIG-ek, a szakaszmérnökségek, továbbá a belvízrendszerek a belvízvédelmi szakaszok határaival, a településekkel, a fő- és mellékcsatornákkal, a főművi szivattyútelepekkel, a belvíztározókkal, a vízvisszatartásra igénybe vehető területekkel, a vízátadási, vízátvételi helyekkel.

A védekezési tervekhez mindig csatolni kell mellékletként a védekezésre kötelezettek részéről a név, cím és beosztás jegyzéket, amely alapja a riasztásnak, kiértesítésnek.

A VIZIG-eknél mindezeken túl évente *Védekezési Szervezeti Beosztást* is készítenek, amely egy komplex adatbázis a védekezésbe bevonandó munkaerőről, technikáról,- fokozatokhoz rendelve őket belvízvédekezéskor is.

Az elkészült *belvízvédelmi terveket* a vízügyi igazgatóságok esetében a felettes szerv az Országos Vízügyi Főigazgatóság hagyja jóvá, ugyanakkor a helyi önkormányzatok és a vízi társulatok esetében a polgármester, ill. az intézőbizottság elnöki jóváhagyás előtt a VIZIG szakmai állásfoglalását is ki kell kérni. A tervek egy példányát a VIZIG részére biztosítani

kell, melyet a szakaszvédelmi központban helyeznek el ezzel is biztosítva a beavatkozások során a szakmaiságot.

Vízkárelhárítási tervek a települések ár- és belvízvédelmében

Az önkormányzatok az elmúlt években a megyei és helyi védelmi bizottságok által a részükre elkészítésre meghatározott *Vízkárelhárítási tervet* az 1991-ben készült, és legtöbbjük részére kiadott "Települési vízrendezési feladatok megoldásához" című útmutató alapján dolgozták ki.

Helyi vízkárelhárítás az árvíz-, belvízvédekezés céljából kiépített védművek hiányában a fellépő káros vizek elleni védekezés, és az elöntések szétterült vizeinek a vízfolyásokba, csatornákba vezetése.

Sajnos az önkormányzatok jelentős része nem készítette el ezt a települési ár-és belvízvédekezés szempontjából alapvető tervet. Az Állami Számvevőszék két alkalommal vizsgálta a települések vízrendezési és csapadékvíz elvezetési feladatellátását 1999-ben és 2007-ben. Az ÁSZ Jelentésében megállapította, hogy a vízkárelhárítási tervek a települések 51%-ban nem készültek el, illetve ahol elkészültek az aktualizálásuk sok esetben nem történt meg.

Javasoljuk, hogy a jövőben a vizek kártételei elleni védekezés feladatait egységes jogi normák határozzák meg, mert az egyébként vitathatatlanul hasznos, a védelmi bizottságok által kezdeményezett és megkövetelt „Vízkárelhárítási tervek” más műszaki tartalommal készültek el, mint amit a hatályos védekezést szabályozó, Miniszteri rendelet előír az Árvízvédekezési, - illetve Belvízvédekezési Tervek tartalmára vonatkozóan.

A korábbi években a belügyminiszter utasítása alapján a BM OKF és területi szervei - együttműködve az illetékes vízügyi szervekkel - felmérték a belterületi vízelvezető rendszerek állapotát, amelynek tapasztalatairól összefoglaló jelentést készítettek és átfogó javaslatot tettek a hiányosságok megszüntetésére.

A feladat eredményes végrehajtása érdekében valamennyi megyei és a fővárosi igazgatóság részére egységes szakmai szempontrendszer került összeállításra, amely a felmérések alapját képezte. A megyékben a veszélyeztetettség figyelembe vételével a legkedvezőtlenebb vízelvezető rendszerrel rendelkező településeken kezdték meg a helyszínbejárásokat.

A felmérés során vizsgálták:

- település típusát (síkvidék, dombvidék, hegyvidék);
- a közműtérképek meglétét;
- vízkár-elhárítási tervek meglétét;
- árkok, műtárgyak állapotát;
- az árkok hosszának tervezett bővítését;
- az árkok és műtárgyak összehangoltságát;
- a zárt rendszerű csapadékvíz elvezető rendszerek hosszát;
- a belterületi vízelvezető rendszerek kapcsolatát;
- a mélyfekvésű területek beépítettségét
- a mély fekvésű rendszerek vízelvezetését.

A felmérés *1173* települést érintett, melyből *276* db (24 %) volt a kritikus. Az országos számadatokból egyértelműen látható volt, hogy a települések negyedénél komoly problémák jelentkeztek, és jelenleg is vannak, amelyek megoldása nem tűr halasztást. Az évek során a belvízi elöntések kialakulása szempontjából az egyik leggyakoribb előidéző ok az árkok és műtárgyak összehangoltságának jelentős hiánya volt. A Belügyminisztérium által elrendelt felmérések bizonyították, hogy átlagosan 24-25%-ban voltak csak megfelelően kialakítva a bel-és külterületi vízfolyások összehangoltság szempontjából. Mindez azt eredményezte sok helyen, hogy hiába volt rendezett, karbantartott árokrendszer egy településen, a belvízveszély

mégis kialakulhatott, mivel a falutól elvezető közcélú vízfolyást netalán már átszántották, vagy nem tartották karban.

A felmérések rámutattak, hogy a települések belvíz-veszélyeztetettségének csökkentéséhez szükséges a költségvetési támogatás, a saját pénzforrások elkülönítése, de az építésügyi engedélyezési jogkör szigorítása is, hogy ne épülhessenek házak mélyfekvésű területekre. A belvíz okozta károk megelőzését segítené elő az elvezető rendszerek még hatékonyabb kialakítása, azok karbantartása. A kormányzati *közmunkaprogram* is eredményesen hozzájárulhat ehhez, de mindezek nem mentesítik a védekezés szervezésére kötelezetteket a Kormányrendelet, és a Miniszteri rendelet előírásainak betartásától, az ott meghatározott feladatok elvégzésétől.

Statisztikai szempontból említést érdemelnek az *utolsó belvízveszélyes évek. 2006*, amikor is egy csapadékos telet követően a hóolvadások után március 15-én 244.000 hektár területet borított belvíz, 34 településen 242 fő kényszerült elhagyni otthonát, mindösszesen 84 településen több mint 1100 épület, és 3200 fő volt közvetlenül veszélyeztetve. Az időközben akkor a Duna, majd a Tisza mentén kialakult súlyos árvízi helyzet miatt május közepén még mindig 96000 hektár volt belvíz alatt hazánkban, melynek közel fele szántó volt, nem kevés mezőgazdasági vízkárt elszenvedve. Elmondható ugyanakkor, hogy a statisztikák szerint az évi 102ezer hektáros elöntés még átlagosnak ítélhető.

Hasonlóan 2006-hoz, a 2010-es év is kimagaslóan nagy belvízi elöntéseket hozott. Ekkor a májusi-júniusi felhőszakadások időszakában a rendkívüli árvízi védekezések mellett 380.000 hektár belvízzel elárasztott területen kellett megküzdeni a védekezőknek.

A bemutatott belvízi elöntések természetesen jelentős erőfeszítést követeltek az állami irányítástól, az önkormányzati vezetéstől, a katasztrófavédelmi, vízügyi, egészségügyi, közlekedési, mezőgazdasági szakigazgatási, és karitatív szervektől, a rendőrségtől, de leginkább a veszélynek kitett lakosságtól. A *tudatos prevenció* az, amivel alapvetően tudunk küzdeni a belvizek kártételei ellen, melynek konkrét feladatait meghatározzák az idézett vízügyi jogszabályok, és a Katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény és végrehajtási rendeletei.

A belvízvédekezés a belvízkárokat elhárító tevékenység

A *védekezés* az élet- és vagyonbiztonság érdekében, jogszabályokban meghatározott keretek között *szervezett operatív tevékenység*, amely a mederből kilépő árvíz, a csapadék és hóolvadás nyomán keletkezett belvíz elleni védekezés műszaki és az államigazgatási feladatok végrehajtását jelenti.[11] A belvíz elleni eredményes védekezés során, az államnak a vízi társulatoknak és az önkormányzatoknak az együttműködése szükséges. A Miniszteri rendelet 2. számú melléklete meghatározza a belvízrendszerek és védelmi szakaszok rendszerét, ahol alapvetően az államnak vannak feladatai. A települések feladatrendszere a települések belterületére, illetve a vízitársulatokkal közösen a *külterületi védekezési munkálatok* megszervezésére is kiterjed, amely alapvetően a következő feladatokat tartalmazza:

- vízkormányzás[2] (pl. tiltók kezelése)
- vízelvezetés csatornával
- víztározás, alapvetően belvízvisszatartást jelent, melynek alkalmazásával a vizet saját területén visszafogják, ami által biztosítják, hogy értékesebb terület vízkárt ne szenvedjen
- esésnövelő szivattyúzás.

A fentiek figyelembe vételével a települési vízrendezésnek, illetve az önkormányzati védekezésnek alapvetően hármas tagozódású feladatot kell ellátni:

[2] A víz célzott irányítása árkok, belvízcsatornák között, továbbá a vízvisszatartása, majd továbbvezetése.

- a felszínen "megállt" csapadékvíz összegyűjtése és rendezett elvezetése a befogadó helyekre,
- magas szintű talajvizek elvezetése és a talajvízszint csökkentése, szabályozása,
- rendkívüli esetben - ha az elvezetés nem lehetséges - beindul az effektív védekezés az együttműködő szervek (pl. tűzoltóság, polgári védelem), közmunkások, lakossági közerő bevonásával. Szükség esetén mentés kitelepítés, szükségelhelyezés szükségellátás.

A *belvíz-védelmi* tevékenységeket a *védelemvezető irányítja*, aki ezen belül összehangolja a védekezésben résztvevő szervezetek munkáját és a főcsatornán folyó védekezésnek alárendeli. Amennyiben a belvízzel elöntött területekről a befogadók (csatornák, tározók, szükségtározók) teltsége miatt a vizek késleltetett vagy szakaszos levezetése nagy területekre fennáll, a vízzel elöntött területek mentesítése a következő sorrendben valósul meg: lakott területek, ipari létesítmények, közlekedési útvonalak, mezőgazdasági területek, egyéb.

A védelemvezető a tevékenysége ellátása során *belvízvédelmi fokozatot rendelhet* el, határozat formájában. A települési vízkárelhárítási terv tartalmazza az adott településre vonatkozóan az elrendelés időszakát és az elvégzendő feladatokat. [11]

Rendkívüli belvízvédekezési készültség:

Ha a VIZIG működési területén a belvízi elöntés olyan méreteket ölt, hogy a belvíz lakott területeket, ipartelepeket, fő közlekedési utakat, vasutakat veszélyeztet és további elöntések várhatók, a vízügyi igazgató – a védelmi bizottság elnökének egyidejű tájékoztatásával – köteles a Törzs vezetője útján a miniszternek javaslatot tenni a rendkívüli készültség elrendelésének kezdeményezésére. Ekkor a belvizek szükségtározására igénybe veendő területeket elő kell készíteni. A szükségtározó igénybevételét a vízügyi igazgató kezdeményezésére, a Törzs vezetőjének javaslatára, a kormánybiztos engedélyezi.

A fentiekben leírt fokozatok azonban csak ajánlásokat tartalmaznak, hiszen a már említett települési vízkárelhárítási tervben kell rögzíteni konkrétan a fokozatok elrendelésének idejét, módját és az ehhez rendelt tevékenységeket. Az együttműködő szervek és szervezetek feladatát is a belvízi fokozatokhoz kell igazítani.

A *belvíz elleni védekezés* hazánk sajátos veszélyeztetettsége miatt, *évszázados múltra tekint* vissza. Az írásból látható, hogy a kialakulása és az ellene való védekezés terén a szakemberek sokat tettek, de ezek a munkálatok sem mindig voltak elegendőek, így is keletkeztek elöntések. A belvíz elleni védekezés sikeres és eredményes végrehajtásának egyik legfontosabb feltétele, hogy a felszíni vízelvezetők funkciójukat ellássák, ehhez pedig szükséges a folyamatos karbantartásuk, tisztításuk. Sajnos ezen a területen a települések többségénél jelentős problémák vannak, a vízelvezető árkok és átereszek karbantartása évek, esetenként évtizedek óta elmaradt, így azok jelentős mértékben telítődtek iszappal és funkciójukat részben tudják ellátni. A települések vezetése a belterületi felszíni vízelvezetést *sok esetben nem súlyának és fontosságának megfelelően kezeli*. Az ingatlan tulajdonosok részére a telkük előtt lévő árok rész és áteresz évenkénti tisztítását helyi rendeletben elő lehet írni és a végrehajtását, pedig ellenőrizni lenne szükséges. Aki nem hajtja végre karbantartást azt szankcionálni lehet, sajnos ezzel a lehetőséggel a települések elenyésző része él. Az önkormányzatok egy része a vízelvezetők fenntartását közmunkások bevonásával végezte el, ami egy járható út. A beinduló közmunkaprogram kiszélesítésével lehetőségük lesz a településeknek a belterületi vízelvezető rendszerek működőképességének helyreállításához forrásokat igényelni.

A *belvíz elvezető rendszerek* funkciójukat csak akkor tudják ellátni, ha folyamatosan karban vannak tartva, a műtárgyak (zsilipek, szivattyúk) pedig működőképesek. A belvízvédelmi rendszerek következő problémás területe *a műtárgyak* működőképességének biztosítása, amelyeknél sok esetben a legnagyobb gondot az okozza, hogy a zsilipek fém

alkatrészeit *ellopják*. Az alkatrészek hiányán túl, a karbantartottság elmaradása is nagyon sokszor problémát jelent, ezen a területen a költségvetési források növelésével lehet előre lépést elérni.

Nagyon sok településen a *külterületi és belterületi vízrendszerek összehangoltságának a hiánya is súlyos probléma*, melynek eredményeként a külterületekről érkező vizek a települések belterületén elöntéseket okoznak. A termelőszövetkezetek megszűnését követően, a magán gazdaságok kialakulásával a mezőgazdasági területeken keletkező vizek elvezetéséről majdnem mindenki megfeledkezett. Az elmúlt években egyre több településen keletkeztek súlyos belvízi problémák a külterületek és belterületek határánál lévő övárkok, illetve a mezőgazdasági területeken lévő külterületi árkok nem megfelelő állapota, esetenként beszántásuk miatt. Ebben kérdésben a települések polgármestereinek lenne szükséges lépni, mégpedig a földhivatalokban a térképtárakból elő lehet keresni a megfelelő térkép szelvényeket, azokon fel vannak tüntetve a külterületi árkok is. Ezt követően a földterület jelenlegi tulajdonosánál kezdeményezni kellene az eredeti állapot visszaállítását. A folyamatba a megyei Mezőgazdasági Szakigazgatási Hivatal Földművelésügyi Igazgatóságát is szükséges bevonni.

A jövőben mindenképpen a *megelőzésre* kell helyezni a hangsúlyt, a településeket keresztező vízfolyások, csatornák, útárkok tulajdonviszonyai alapján a fenntartási, fejlesztési feladatok megoszlanak, az állam a vízi társulatok és az önkormányzatok között. Ezen túlmenően szükséges lesz többet fordítani a belterületi vízelvezető árkok és a befogadók karbantartására, a műtárgyak rendeltetésszerű funkciójának biztosítására. Ez azért is fontos mivel a globális felmelegedés következtében egyre többször kell számolnunk szélsőségesen sok csapadék mennyiséggel. A hatékony vízelvezető rendszerek kiépítéséhez a szükséges *forrásokat* a települések hazai és uniós pályázati forrásokból tudják biztosítani, a kétkezi munkaerőt pedig a megújuló közmunkaprogramból.

A *gyakorlati feladatok* terén a települési önkormányzatok és vízi társulatok belvíz védekezési feladatait vizsgáltuk, valamint a belvízvédelmi fokozatok elrendelésének kritériumait és a végrehajtandó védekezést. A belvíz elleni szervezett védekezési tevékenység két, jól elkülöníthető része közül ez a *védekezés műszaki feladatainak szervezését, irányítását* foglalja magában.

Ez a védekezés időszakában a védművek ellenőrzését, védelmi teljesítőképességük megőrzését, azaz szükség esetén a terheléssel szemben lokálisan fellépő védőképességi hiányosságoknak a védekezési munkával, ideiglenes védelmi létesítmények kiépítésével való pótlását jelenti.

Másik részük a védekezés államigazgatási feladatainak szervezésére, irányítására és ellátására irányul. A belvíz elleni védekezés védelmi igazgatási feladatrendszerének és jogszabályi hátterének változása és összetettsége miatt egy másik cikk keretében lehet vizsgálni.

7. ÖSSZEGZÉS

Magyarország sajátos helyzetéből adódóan a települések és az egyes emberek kiszolgáltatottságát a vizek kártételei ellen csakis közös összefogással lehet elfogadható mértékűre csökkenteni. Ehhez szükséges az állami, önkormányzati szerveknek, vízi társulatoknak és az egyes embereknek is a maguk területén lépéseket tenni. A *legjobb belvíz elleni védekezés a megelőzés*, úgy gondoljuk ezt az örök értékű megállapítást ezen a területen is kiemelten figyelembe kell venni. A lakott területek belvíz-mentesítése érdekében a település szerkezeti és településrendezési tervek készítésekor, módosításakor kiemelt figyelmet kell fordítani a domborzati és talajviszonyokra. A belterületi felszíni vízelvezetés tervezésekor figyelembe kell venni a mélyfekvésű, elfolyás nélküli területeket, valamint a

külterületi és belterületi vízelvezetők összehangolását**.** Hazánkban az egyik legnagyobb katasztrófavédelmi kihívás napjainkban *a rendkívüli ár- és belvíz elleni védekezés megszervezése és végrehajtása*. A rendkívüli időjárás okozta elöntések, belvizek elkerülése érdekében nagyon fontos az árkok vízelvezető képességének a megőrzése, ez pedig a rendszeres tisztítással és karbantartással biztosítható. Ehhez a civil szférának és az önkormányzatoknak is minden tőlük telhetőt meg kell tenniük, ahogy az új katasztrófavédelmi törvény is fogalmaz**,** a katasztrófavédelem nemzeti ügy. [10]

Cikkünkben a *belvíz kialakulását és az ellene való védekezés* összetett problémáját vizsgáltuk. Hazánk földrajzi adottságaiból adódóan és az időjárás várható szélsőségesebbé válásának következtében, az elkövetkező években is számolhatunk kisebb-nagyobb belvízi elöntések kialakulásával. Mindenképpen szükséges a belvízvédelem rövid és középtávú stratégiájának újragondolása, melyben az állami szerepvállalásnak meghatározónak kell lennie és a jövőkép szempontjából nem mellékes a belvizek kérdését együtt vizsgálni a vízmegtartás témakörével.

Felhasznált irodalom

[1] Dr. Koncsos László, Balogh Edina: Belvízkockázatok számítása korszerű hidroinformatikai eszközökkel; http://www.hidrologia.hu/vandorgyules/27/dolgozatok/04koncsos-balogh.htm; (2011. 11. 27.)

[2] Ismerettár: Belvíz; http://www.vkki.hu/index.php?mid=350; (2011. 11. 27.)

[3] Dr. Bíró Tibor: A belvíz kialakulásának térinformatikai elemzése; http://www.otk.hu/cd19xx/1999/szek1/birotibor.htm; (2011. 11. 26.)

[4] Dr. Rakonczai János, Csató Szilvia, Dr. Mucsi László, Kovács Ferenc, Szatmári József: Az 1999. és 2000. évi alföldi belvízelöntések kiértékelésének gyakorlati tapasztalatai http://www.geo.u-szeged.hu/web/sites/default/files/publikaciok/ML/55.pdf; (2011. 11. 27.)

[5] Forgóné Nemcsics Mária PhD értekezés: Belvízkár elhárító rendszerek fejlesztésének mezőgazdasági megalapozása földrajzi információs rendszerrel; http://www.szie.hu/file/tti/archivum/Forgoe_phd.pdf; (2011. 11. 28.)

[6] Dr. Zsembeli József: Vízrendezés drénezés Debreceni Egyetem Mezőgazdaság Tudományi Kar; http://www.agr.unideb.hu/ktvbsc/dl2.php?dl=62/4_eloadas.ppt; (2011. 10. 28.)

[7] 1995. évi LVII. törvény a vízgazdálkodásról

[8] 232/1996. (XII. 26.) Korm. rendelet a vizek kártételei elleni védekezés szabályairól

[9] 10/1997. (VII. 17.) KHVM rendelet az árvíz- és a belvízvédekezésről

[10] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról

[11] Petró Tibor: A helyi vízkár elleni védekezés helyzete napjainkban, a védekezés feladatai Hadmérnök VI. évfolyam I. szám 2011. március (177-179. o.)

[12] Muhoray Árpád pv ezredes, A katasztrófavédelem területi irányítási modelljének vizsgálata, doktori(PhD) értekezés 2002, Zrínyi Miklós Nemzetvédelmi Egyetem ‚Doktori Iskola/ 82.oldal

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Meglécz Katalin
meglecz.katalin@hm.gov.hu

A PANDÉMIÁK TÖRTÉNETE ÉS KIALAKULÁSUK OKAI

Absztrakt

A 2009-2010. évi influenza pandémia rávilágított a járvány, mint a katasztrófát kiváltó ok fontosságára. A megfelelő ismeretek a potenciálisan bekövetkező újabb világjárványok megelőzéséhez, gyors felismeréséhez, elterjedésének megakadályozásához és felszámolásához szükséges intézkedések alapját képezik. A cikk a történelem nagy járványai, mint a pestis, kolera, himlő és influenza által okozott világjárványok tapasztalatait vizsgálja

The influenza pandemic in 2009-2001 has highlighted the endemic as an important cause of disaster. The article examines the experience of the history of major epidemics such as plaque, cholera, smallpox and influenza. A proper knowledge gives the base of necessary measures to prevent, quick detect, hinder of the spread and eliminate the pandemic potentially occur in future.

Kulcsszavak: *pandémia, pestis, himlő, influenza, kolera, katasztrófa ~ pandemic, plaque, smallpox, influenza, cholera, disaster*

1. BEVEZETÉS

Az elmúlt két évben a katasztrófák sorában ismételten kiemelt jelentőséget kaptak a járványok, járványügyi katasztrófák. A XX. században az orvostudomány fejlődésével, a betegségek hatékony megelőzési stratégiáinak, a közegészségügyi-járványügyi intézményrendszernek és rendszabályoknak világméretű elterjedésével, a védőoltások bevezetésével csökkent a fertőző megbetegedések szerepe a fejlett világban. Ennek köszönhetően a katasztrófa szó hallatán elsősorban természeti jelenségekkel összefüggő események – földrengés, szökőár, földcsuszamlás, esetleg ipari katasztrófák képei villannak fel.

A 2009-2010 influenza pandémia bebizonyította, hogy a fertőző megbetegedésekkel és az általuk okozott világméretű járványokkal mind a mai napig és a jövőben is komolyan számolnunk kell. A folyamatok megismerése, a felkészülés és védekezés hatékonysága érdekében elengedhetetlen a pandémiák történetének ismerete.

Az alábbiakban a legnagyobb jelentőségű pandémiás megbetegedések történetét tekintem át.

2. EPIDÉMIA, ENDÉMIA ÉS PANDÉMIA

A történeti áttekintés pontos megértéséhez szükségesnek tartom az alapvető járványügyi fogalmak tisztázását.

A *fertőző betegségnek* nevezzük azokat a betegségeket, melyeket specifikus fertőző ágens, vagy annak terméke hoz létre, és amelyek képesek közvetlenül, vagy közvetve emberről emberre, állatról emberre, állatról állatra terjedni.

A fertőző betegségek többféle formában fordulhatnak elő. *Sporadikus*nak nevezzük akkor, ha az egyes esetek elszórtan, egymástól függetlenül fordulnak elő, közöttük a kapcsolat nem kimutatható. Ha egy fertőző betegség rövid időn belül nagy számban, tömegesen fordul elő és az esetek között kapcsolat mutatható ki *epidémiáról* (járványról) beszélünk. Amennyiben egy adott területen az adott fertőző megbetegedés állandóan, tartósan jelen van, *endémiáról* beszélünk. *Pandémiának* a világjárványokat nevezzük, amikor a járvány több földrészre, akár az egész világra kiterjed [1].

3. PESTIS

A pestis világszerte előforduló Yersisnia pestis baktérium által előidézett, vektor által terjesztett fertőző megbetegedés. A pestist a fertőzött állatról, igen ritkán a fertőzött emberről a leggyakrabban a patkánybolha (Xenopsylla cheopsis) vagy más bolha viszi át emberre. Beteg állattal történt közvetlen érintkezés, beteg állat harapása által is előfordultak emberi megbetegedések. A leggyakrabban a vándor- és házipatkány a rezervoár, de mintegy 370 állatfaj képes fenntartani a pestis-baktériumot a természetben. A betegség másik formája a tüdőpestis cseppfertőzéssel terjed.

A betegség hirtelen magasra emelkedő lázzal, zavartsággal, delíriumig fokozódó nyugtalansággal kezdődik. Mivel a kórokozó leggyakrabban bolha csípése révén kerül az ember szervezetébe, ennek következtében ún. bubopestis fejlődik ki, azaz a behatolási kapuhoz közeli nyirokcsomó megnagyobbodása, gyulladása jön létre. A betegség lappangási ideje 2-5 nap. A bubopestises betegek egy részénél a folyamat generalizálódik, a septicaemia következtében pestis-pneumonia fejlődhet ki. A kezeletlen betegek letalitása 60%, a legtöbb haláleset 3-5 nap alatt halához vezet, melynek elsősorban szepszis az oka.

A tüdőpestis járványügyi jelentőségét az adja, hogy a beteg már nem csupán a bolha közvetítésével, hanem közvetlenül, cseppfertőzés révén is fertőzőképes: a környezetében lévő

személyeknél elsődleges tüdőpestis alakulhat ki, amely kezelés nélkül 2-3 nap alatt halálhoz vezet, letalitása mintegy 100%. A kezelt pestis halálozási aránya 5 % [2].

A pestis a kiemelten kezelendő úgynevezett karantén betegségek egyike. Előfordulásakor kiemelt járványügyi intézkedésekre kerül sor a közösség és az egyén védelmében. Az esetet az Egészségügyi Világszervezetnek is jelenteni kell.

Ázsiai területeken hagyományosan endémiás (tartósan, rendszeresen előforduló) volt, de más földrészek természeti gócaiban is rendszeresen előfordult, előfordul. A pandémiák létrejöttében nagy szerepe volt a kialakult népmozgalmaknak, a tengerhajózás és nemzetközi kereskedelem fejlődésének, és a háborúknak is [3]. A pestis a patkányok és a patkánybolhák révén honosodott meg az észak-afrikai és európai kikötővárosokban, és terjed át az amerikai kontinensre is. A pandémiák közül a VI., XVI., XIX.-XX. századi pandémiák jártak a legtöbb áldozattal. A becslések szerint a pestis Európában 25 millió áldozatot szedett.

Az utolsó pandémia 1894-ben Hong-Kongban kezdődött és patkányok réven terjedt. Az 1894-1934. években a pandémia kb. 13 millió halálesetet okozott Indiában, Kínában és Dél-Kelet Ázsiában, 120 ezret Afrikában, kb. 25 ezer haláleset fordult elő az amerikai kontinensen, és 1000 Európában. Magyarországon az utolsó járvány az 1737-1751-es években fordult elő Hajdú-Bihar, Szabolcs-Szatmár, Szolnok és Csongrád megyében [4].

A pestis ma már csak a rossz higiénés körülményekkel rendelkező trópusi és szubtrópusi országokban jelenik meg. Ilyen országok, pl. India, Vietnam vagy Madagaszkár, ahol négy egymást követő évben is észleltek járványt. Általában hűvösebb, nedves klímájú területeken fordul elő pestis. A fejlettebb országokban, ahol a patkányok nem fertőzöttek, ott a betegség sem fordul elő. Az Egyesült Államokban az emberi pestis megbetegedések több mint 90%-a a délnyugati államokban, Arizonában, Kaliforniában fordul elő [5]. A természetes járvány kialakulásának valószínűsége mára igen csekély.

4. KOLERA

A kolera a Vibrio cholerae által okozott heveny enterális fertőző megbetegedés. A betegség lappangási ideje 1-3 nap. A típusos, súlyos klinikai tünetek, a gyakori rizslészerű széklet ürítése, hányás, súlyos kiszáradás, vérnyomásesés, veseműködés zavara a klasszikus kórokozó esetében mintegy 20 %-ban, az utóbbi időben, a hetedik pandémia során teret nyert El Tor variáns estében 1-4 %-ban jelennek meg. A fertőzések többsége enyhe, tünetszegény formában jelentkezik. A betegség emberről-emberre elsősorban széklet, hányadék, valamint az ezekkel szennyezett víz és élelmiszerek útján terjed. A súlyos kolerában szenvedő kezeletlenek több mint 50%-a meghal. Azonnal megkezdett, megfelelő folyadékpótlás esetén a betegek kevesebb, mint 1%-a hal meg.

Mai ismereteink szerint a kolera Ázsiában, Indiában és Pakisztán területén az ie. V. századtól honos fertőző megbetegedés, amely Ázsia határain belül évszázadokon át járványosan terjedt el. 1817-ben a kolera kitört e területekről és világméretű járványos elterjedése következett be.

Hét kolera pandémiát jegyeztek fel, azt első 1817-1823.-ig, a második 1828-1837.-ig, a harmadik 1844-1864.-ig, a negyedik 1865-1875.-g, az ötödik 1883-1896.-ig, a hatodik 1900-1926.-ig zajlott. A hetedik kolera pandémia 1961-ben kezdődött és jelenleg is tart.

Magyarországon két alkalommal okozott a kolerajárvány nagy pusztítást: 1832-1833-ban és 1872-1873.-ban. A megbetegedettek száma mindkét esetben meghaladta az 500 ezer főt, és mivel a halálozási arány ekkor 50-60 % volt, az első járványban meghaltak száma meghaladta, a másodikban megközelítette a 200 ezer főt.

Az első három pandémia szárazföldön a karavánok útvonalát követve, majd a nagy folyók mentén terjedt el. A negyedik, ötödik és hatodik pandémiánál a tengerhajózás játszott fontos szerepet, a hetediknél a légiközlekedés volt a terjedés fő mozgatórugója.

Megemlítendő, hogy csupán a második és negyedik pandémia idején terjedt el a kolera járványosan az amerikai kontinensen [6].

A hetedik pandémia Ázsia egyes részeiben, Közép-Keleten, Kelet-Afrikában és Latin-Amerikában mind a mai napig járványokat okoz. A Haiti földrengést követően kialakult kolerajárványban az elmúlt évtized legjelentősebb járványává nőtte ki magát. Azonban a hetedik pandémia segítette hozzá az orvostudományt a betegség patomechanizmusának megértéséhez, a folyadékpótlás hatékony módjának kidolgozásához, valamint a védőoltás kifejlesztéséhez [7].

5. HIMLŐ

A feketehimlő a Poxvirus variolae által okozott, heveny, ragályos betegség. A kórokozó a Poxviridae család Orthopoxvírus nemzetségébe tartozik. A nemzetséghez sorolják a tehénhimlő, a tevehimlő és a majomhimlő vírusát is. A betegség cseppfertőzéssel terjed, és fogékony populációban rövid idő alatt nagyszámú, súlyos, nagy számban halálos megbetegedést okoz. Egyetlen eset előfordulása járványveszélyt jelent.

A betegségnek két fő formáját figyelték meg: Variola major (vera), a letalitás 20-40%, vagy ennél magasabb. Variola minor (alastrim), melyet a variolavírus gyengébb virulenciájú változata okozott. A kórkép megfelel a variola verának, de annál jóval enyhébb lefolyású, a letalitás 1% alatti. A betegség ritka, de minden esetben halálos végű formája a primer haemorrhagiás variola.

A himlő heveny klinikai tünetei vírusfertőzésre, leginkább influenzára emlékeztetnek, többnyire hirtelen kezdet, magas láz, fejfájás, szédülés jellemzi a prodromális szakot. A kezdeti tünetek után két-három nappal a láz leesik, és megjelennek a kiütések. A bőrelváltozások szabályos fejlődést mutatnak: előbb gombostűfejnyi lapos foltocskák jelennek meg, amelyek később papulává nőnek, majd vesiculává alakulnak. Az 5. napra a hólyagocska benneke zavarossá válik és kialakul a himlős pustula. Az orr és a száj nyálkahártyáján megjelenő elváltozások kifekélyesednek, ennek következtében nagymennyiségű vírus jut a szájba és a torokba, amely révén a továbbterjedés hatékonysága megnő.

A himlő ie. 1000-ben már endémiás volt Indiában, később Kínában is. Európa nagy részén csupán a VI. század végén jelenik meg a himlő, mely a XIII.-XVI században vissza-visszatérő, gyilkos járványokat okozott. A betegség letalitása 10-30 % között ingadozott, a lakosság túlnyomó többsége átesett a betegségen, így becslések szerint a XVIII. században mintegy 60 millióra tehető a himlő következtében meghaltak száma [8].

A legnagyobb jelentősége Amerikában a hódítások korában következett. Az aztékok és a spanyol hódítók első érintkezésest követően borzalmas himlőjárvány tört ki az indiánok között, ami alapjaiban roppantotta meg a birodalom katonai és gazdasági erejét, így Cortes hódítása nem ütközött ellenállásba. Peruban a járvány már megelőzte a spanyolokat - az inka birodalmat ezek után egy maroknyi konkvisztádor is térdre kényszeríthette. A himlő (az első számú, de nem az egyetlen behurcolt ragályos betegség - hogy csak a kanyarót és az influenzát említsük) kiirtotta a Karib-szigetek teljes őslakosságát: egyedül Mexikóban milliókat ölt meg alig néhány évtized alatt, s százezres nagyságrendű volt a halottak száma a volt inka birodalomban is. Az európaiak térfoglalásával (plusz az afrikai rabszolgák letelepítésével) újabb népcsoportokat hódoltatott be: a préríindiánokat például az 1837-38-as epidémia tizedelte meg - ekkor már az amerikai kormányzat oltani kezdte a lakosságot [9].

Az észak-amerikai függetlenségi háború eseményeit a csapatok között mindkét oldalon pusztító himlő folyamatosan befolyásolta. A korábban már megszállt északi gyarmatokat a függetlenségiek, a tömeges megbetegedések miatt nem tudták megtartani és az Egyesült Államokhoz csatolni, így Kanada, amely brit koronagyarmat maradt, mai függetlenségét a

himlőnek köszönheti. A járványnak végül a Washington elnök által elrendelt variolizáció vetett véget [10].

A himlő az egyetlen világszerte felszámolt fertőző betegség. Az erre irányuló vakcinázási akció előtti évben, 1967-ben, a járvány mintegy 10 millió embert fertőzött. A kampány lényegében Jenner módszerén alapult, és 1980-ban hivatalosan lezárult. A siker azon alapult, hogy ez egy igen konzervatív, nagyon kevéssé változékony vírus, amely csak emberben képes fertőzni és szaporodni, és nem okoz lappangó vagy perzisztens fertőzéseket.

Az utolsó természetes úton szerzett himlő megbetegedés 1977 októberében Szomáliában fordult elő. A globális eradikációról szóló bizonyítványt két évvel később írták alá, melyet 1980 májusában az Egészségügyi Világszervezet Közgyűlése is deklarált [10].

Mivel a himlővírusa eltűnt a földről, a laboratóriumokban tárolt himlő víruskészletek megsemmisítését határozta el a WHO, majd 1999-ben a WHO a himlővírus megsemmisítésének határidejét 2002-re halasztotta, és tárolását csak az USA-ban (a Centers for Disease Control and Prevention-ban) és Oroszországban (a Virológiai és Biotechnológiai Kutatóközpontban) engedélyezték. A WHO közgyűlése az idei évben a készletek tárolását további 3 évre (2014-ig) engedélyezte a két laboratóriumnak [9].

6. INFLUENZA

A klasszikus világjárványok kórokozói közül az influenza vírusok maradtak azok, melyek változatlanul évről-évre a legnagyobb számú megbetegedést okozzák világszerte. Az influenza vírus antigénjeiben rendkívül változatos, így időszakonként újabb és újabb variánsok bukkannak fel, amelyek ellen a lakosság nagy része nem védett, még nem alakult ki ellenük a szervezet saját védekező rendszere, így rendkívül fertőzőképesek.

Az influenzára jellemző, hogy nagyon gyorsan fejlődik ki, akár néhány óra alatt megbetegedhet valaki, a kezdeti tünetek általánosak, a levertség, izomfájdalom és a láz. A banális megfázással ellentétben az influenza súlyos szövődményekkel és betegségekkel járhat. A leggyakoribbak a tüdő- és hörgőgyulladás, középfülgyulladás, orrmelléküreg-gyulladás, de akár szívizomgyulladás, agyvelőgyulladás és agyhártyagyulladás is felléphet. Az influenza neurológiai és mentális szövődményeket, sőt halált is okozhat. Becslések szerint a XX. században több mint 50 millió ember halt meg influenzában vagy annak szövődményeiben.

Az influenza vírusok speciális tulajdonságaik révén felelnek meg a világjárványt potenciálisan kiváltó kórokozók feltételeinek.

Az influenza kórokozói az A, B és a C influenza vírusok. Kiterjedt járványokat, pandémiákat az A vírus okoz. A B vírus csak kisebb esethalmozódásokat, a C pedig ritkán egyedi eseteket okoz. Az A vírus a természetben két nagy változatban fordul elő, humán (emberi) és avián (madárinfluenza) törzsek ismeretesek.

Az A vírusok felszíni struktúráját meghatározó antigének a haemagglutinin (H), a neuraminidáz (N). A H antigén a vírus patogenitásában játszik döntő szerepet, az N antigén a vírusnak a fertőzött sejtekből való kilépését, szóródását segíti elő. Összesen 16 H és 9 N antigént ismerünk, közülük az emberi megbetegedést okozó törzsekben három H (H1, H2, H3) és két N antigén (N1, N2) fordul elő. Az avián influenzavírusokban mind a 16 H és a 9 N antigén egyaránt előfordulhat. Itt a következő antigénstruktúrák a legismertebbek: H5N1, H9N2, H7N7, H9N2, H7N2, H7N3.

Az A vírus felszíni antigénjei folyamatos változásban vannak. A változás általában lassú és részleges (drift), de lehet gyors és teljes is (shift). A drift pontmutáció következménye. Ritkább a gyors változás (shift), amikor is a felszíni antigének hirtelen lecserélődnek. Ekkor a replikáció során a vírus genetikai állományába új, rendszerint madárinfluenza-vírus eredetű komponens épül be. Az új, megváltozott antigénszerkezetű kórokozóval szemben pedig a népesség korábban megszerzett immunitása hatástalan, ami pandémia kialakulásának

veszélyét teremti meg. A B vírusnál az antigének változékonysága lényegesen kisebb, a C vírus esetében pedig elhanyagolható. Az 1977 óta időről-időre visszatérő járványokban a humán H1N1 és a H3N2 A vírusok, illetve a B influenzavírusok a globálisan elterjedt kórokozók [11].

A humán influenza megbetegedések járványos előfordulásairól négy évszázadra visszamenően vannak feljegyzések. A pandémiák kialakulása 30-40 évenkénti periodicitást mutat. A XIX. században legalább 4 nagy pandémia zajlott le.1918-ban indult a XX. század első nagy járványa, a „spanyolnátha", amely korunk egyik legnagyobb biológiai katasztrófája volt. Az I. Világháború után tört ki, a Föld lakosságának 20-40%-át betegítette meg és az áldozatok száma jóval 20 millió felett volt, de egyes becslések szerint elérte a 100 milliót is. A betegség jórészt vérzéses tüdőgyulladás képében alakult ki, és rendkívül gyorsan, órák alatt halálhoz vezetett. A vírusos pneumónia különösen a 20-40 éveseket sújtotta szokatlanul nagy számban. Az idősebbek között és a kockázati csoportokban - idült kórállapotokban, anyagcsere-betegségekben szenvedők stb. - inkább a másodlagos, bakteriális pneumónia bizonyult gyakoribb haláloknak A vírus felszíni antigénstruktúráját H1N1-nek tartják, ezt reverz genetikai módszerek alkalmazásával, 80 év után sikerült rekonstruálni [12].

A spanyolnátha elnevezés eredete egyfelől az volt, hogy először Spanyolországban írták le az új megbetegedést, másrészt pedig más országokban nem közöltek jelentéseket az áldozatok és fertőzöttek számáról.

A vírus a 20-40 éves korosztályt érintette leginkább. Ennek oka valószínűleg kettős lehetett, egyrészt az, hogy az érintett korosztály valószínűleg ezt megelőzően még nem találkozott a vírussal, míg az idősebbeknek lehetett fennmaradó immunitása előzetesen átvészelt influenzás megbetegedések révén, másrészt az I. világháborúban az érintett korosztály vett aktívan részt életkorából adódóan. A frontszolgálattal járó minimális higiénés követelmének hiánya, zsúfoltság, alultápláltság, legyengült immunrendszer mind kedveztek a betegség viharos lefolyásának. Az áldozatok többsége a feljegyzések szerint 24 órán belül halt meg. A spanyolnátha járvány elősegítette a világháború befejezését is, mivel a járványban többen haltak meg, mint a harcokban, melyhez a katonák túl betegek voltak.

A spanyolnáthát követően is fordultak elő influenza pandémiák:

1957-ben az „ázsiai influenza"-nak nevezett nagy pandémia alakult ki, a kórokozót hamarosan azonosították (H2N2). Mivel vele szemben kizárólag a 65 éven felüliek rendelkeztek némi immunitással a járvány hamarosan pandémiába csapott át. A spanyol influenzához képest jóval kisebb halálozással járt.

1968-ban a járvány az év elejétől 1969 tavaszára is áthúzódott. A megbetegedések súlyossága elmaradt a korábbiakhoz képest, ami azzal magyarázható, hogy a kórokozóval szemben (H3N2) az előző járványban szerzett immunitás némi keresztvédelmet nyújthatott.

1976-ban riadalmat keltett, hogy az USA egy katonai bázisán a betegekből „sertés influenza" vírust izoláltak, ezt a vírust a spanyolnátha kórokozójával hoztak kapcsolatba. Járvány akkor nem alakult ki.

1977-ben zajlott az „orosz influenza". A H1N1 törzs visszatérésével és elterjedésével sajátos járványhelyzet állt elő. Tekintélyes számú megbetegedés történt ugyan, de kizárólag azon fiatalok között, akik 1957 után, az addig domináló H1N1 eltűnését követően születtek.

1997-tõl új helyzet alakult ki. A korábban csak állatorvosi körökben ismert madár (avián) influenza vírusok Hongkongban hatalmas pusztítást végeztek a csirkeállományban és a H5N1 törzs súlyos humán betegséget is okozott, 18 egyén megbetegedett, és 6 meghalt [13]. Feltételezik, hogy az avián törzseknek korábban is volt szerepük pusztító pandémiák előidézésében [12].

Az új évezred elején szakemberek egy madárinfluenza-világjárványtól tartottak [14], de végül is nem ez történt. 2009 áprilisában kezdődött egy gyorsan globálissá váló H1N1 influenzajárvány, melyet a WHO 2009 júniusában pandémiának minősített. A pandémia első

hullámának végét 2010 februárjában nyilvánították befejezettnek. Ezen időszak alatt a pandémiával megerősítetten összefüggő halálesetek száma világszerte meghaladta a 18 400 főt [15].

7. PANDÉMIÁK KIALAKULÁSÁNAK OKAI

Egy járvány elterjedéséhez három feltétel szükséges: a fertőző forrás, a kórokozó terjedését lehetővé tevő környezeti tényezők és körülmények, valamint az adott fertőző megbetegedéssel szemben fogékony szervezet. A történelemben pandémiát okozó megbetegedések eredetileg endémiásak voltak, tehát a fertőző forrás adott volt. A járványfolyamat másik két eleme közül a fogékony szervezetek is rendelkezésre álltak, hiszen az endémiás területeken kívül más területeken, földrészeken az adott betegség ismeretlen volt. Az általam bemutatott fertőző megbetegedések által okozott világjárványok vizsgálatából is kitűnik, hogy második tényező – a kórokozó terjedését biztosító körülmények és környezeti tényezők közbelépése – kellett ahhoz, hogy egy endémiás betegségből epidémia, majd pandémia alakulhasson ki.

Az ismertetett példákon keresztül megfigyelhető, hogy a pusztító járványok törvényszerűen akkor törnek ki, ha egy területen hirtelen megnő a társadalmi mozgás, vagyis, ha felgyorsul a közlekedés, megélénkül a kereskedelem, egész népcsoportok változtatnak lakóhelyet. A kiépített úthálózat, a kereskedelem fellendülése kedvezett a kórokozók gyors elterjedésének, miközben az emberek immunrendszere képtelen volt ilyen rövid idő alatt alkalmazkodni ezekhez. A lakosság pánikreakciói legtöbb esetben még növelték a bajt: a városokból, táborokból a betegség elől menekülők szertevitték a kórokozót az attól addig mentes területekre is [3].

A *kereskedelem fellendülése*, mint a pandémiát kiváltó ok megfigyelhető a kolera járványok esetében, ahol előbb a karavánútvonalak mentén terjedt a betegség. A későbbi kolera pandémiák és pestis fertőzések a kereskedelem új útvonalának és közlekedési formájának, a tengerhajózásnak elterjedésével indultak útjukra.

A *közlekedés fellendülése*, az előbb említett tengerhajózás, de különösen a légi utas szállítás, mint egy következő ok játszott szerepet a hetedik kolera pandémia, valamint az influenza 1957 évet követő világjárványainak, de különösen a 2009. évi influenza A H1N1 pandémia kialakulásában, és gyors elterjedésében.

A történelem minden szakaszára jellemző, hogy a háborúk és a járványok együtt jártak, összefüggtek egymással. A hadjáratokat rendszeresen járvány kísérte, és igen gyakran a győzelmet is az döntötte el, hogy melyik fél seregét sújtotta kevésbé. Ráadásul egészen a XX. századig megfigyelhető az is, hogy a járványok áldozatainak száma mindig messze meghaladta a hadi eseményekben meghaltakét. Nagy hódítók, köztük Xerxész, Nagy Sándor, Napóleon kényszerültek visszavonulásra betegségtől tizedelt seregük roncsaival. Az összefüggés oka a tömeges migráció, infrastruktúra túlterheltsége, majd összeomlása, zsúfoltság, összezártság a táborokban, élelmezés, személyi higiéné elégtelenségében és az egyes egyének immunrendszerének leromlásában keresendő.

Az általam leírt spanyolnátha pandémia kitűnő példája a *háborúk*kal ok-okozatként összefüggő, azok kimenetelét befolyásoló járványokra.

A nagy felfedezések korában, a XV. századot követően védettséggel nem rendelkező emberek jutottak el nagy tömegben egyes megbetegedések endémiás területeire, megbetegedtek, majd a betegséget továbbhurcolták. A járványok kialakulásának másik – ezzel ellenkező előjelű – folyamata olyan emberek megjelenése számukra idegen területen, földrészeken, akik magukkal vittek egy ott addig ismeretlen megbetegedést, amely a helyi lakosságot tizedelte meg, és meghonosította az adott betegséget. A leírt himlő járványok kiváló példái a *hódítások*nak, mint a pandémia kiváltó okának.

A nagy járványoknak valószínűsíthetően a magas halálozások kiváltotta hirtelen népességcsökkenés, a természetes szelekció és az immunizálódás vetett véget. A következő pandémia akkor indulhatott, amikor ismét megjelent a nagy számú fogékony népesség, vagy a kórokozó változott. Ez adja a pandémiák ciklicitását.

Meglepő lehet, de a járványoknak köszönhetők pozitív hatások, változások is. Például az elsősorban a fertőzött ivóvíz és általában a rossz higiénés viszonyok miatt terjedő kolera hatására kezdték el az európai nagyvárosok - London mintájára - kiépíteni csatornahálózatukat, vízvezeték-rendszerüket, közegészségügyi, köztisztasági szervezeteiket. Hatására terjedtek el a - korábban is ismert - angolvécék, derítők, fürdőszobák, ennek nyomán kezdtek el többet foglalkozni a lakások tisztaságával [7].

A hadi- és a közegészségügy megszervezésének szükségességét is a kolerajárványok miatt látták be, miatta foglalkoztak egyre többen bakteriológiával és virológiával, és epidemiológiával is.

Európában - és az egész világon - az utolsó nagy hatású járvány az 1918-as spanyolnátha-járvány volt, amelynek 30 millió áldozata volt. Ez a járvány hívta fel a figyelmet a nemzetközi egészségügyi együttműködés fontosságára [16].

Ma a pandémiák kialakulásának megelőzése érdekében a természetben előforduló gócok – fertőző források, és fogékony egyedek közti kapcsolat, a második tényező, azaz a terjedési mechanizmus kiiktatásán dolgoznak a közegészségügyi szakemberek hazánkban és világszerte, ezt biztosítja a közegészségügyi rendszabályok, előírások rendszere. Az esetlegesen előforduló egyes megbetegedések járvánnyá fokozódását már a korai szakaszban az egészségügyi rendszabályok betartása megakadályozza, az embert, mint fertőző forrás kiiktatását a rendszerből a gyors klinikai diagnózis és adekvát kezelés segíti. A kötelező és fakultatív védőoltások rendszere pedig a fogékony szervezetek számának csökkentésében játszik szerepet.

8. ÖSZEFOGLALÁS

A 2009-2010. évi influenza (A) H1N1 pandémia következtében a járványok, mint katasztrófát potenciálisan kiváltó események újra előtérbe kerültek. A történelmet befolyásoló, jelentős pandémiákat okozó négy fertőző megbetegedés példáján keresztül vizsgáltam a világjárványok kialakulásának lehetséges tényezőit.

Megállapítottam, hogy a pandémiák létrejöttében a járványfolyamat első és harmadik eleme, a fertőző forrás és fogékony szervezetek rendelkezésre álltak. A második elem, a kórokozó terjedését biztosító környezeti tényezők és körülmények kellettek a betegségek hatékony, gyors és világméretű elterjedéséhez. Ezek a feltételek a kereskedelem és közlekedés fejlődésével és a háborúk, hódítások térnyerésével erősödtek meg és vezettek a pandémiák kialakulásához.

A mai globalizált világ kiváló táptalaja lehet a világjárványok létrejöttének, azonban a megelőző egészségügyi rendszabályok betartásával, fertőző források kiiktatásával valamint a fogékony szervezetek immunizálásával a járványok kialakulásának valószínűsége csökkenthető.

Felhasznált irodalom

[1] Nagylucskai Sándor: A fertőző betegségek járványtana pp.79-80 in: Dési Illés (szerk.) Népegészségtan, Semmelweis Kiadó, Budapest, 1999

[2] Nagylucskai Sándor: A fertőző betegségek részletes epidemiológiája pp. 167-168 in: Dési Illés (szerk.) Népegészségtan, Semmelweis Kiadó, Budapest, 1999

[3] Magyar László András: Morbid Történelem - Historia morbida c. előadása; Történelemtanárok 14. Országos Konferenciája, 2004. http://www.tte.hu/toertenelemtanitas/toertenelemtanarok-orszagos-konferenciaja/6722-morbid-tortenelem-historia-morbida; (2011. 10. 20.)

[4] Vedres István: Bacterialis és vírusfertőzések. Pestis. pp. 575-579. in Fodor Ferenc – Vedres István (szerk.) A közegészségtan és járványtan alapjai, második kiadás, Medicina Budapest, 1975

[5] CDC map World Distribution of Plaque 1998; http://www.cdc.gov/ncidod/dvbid/plague/world98.htm; (2011. 06. 10.)

[6] Vedres István: Bacterialis és vírusfertőzések. Cholera (cholera asiatica, kolera) pp. 500 - 505. in Fodor Ferenc – Vedres István (szerk.) A közegészségtan és járványtan alapjai, második kiadás, Medicina Budapest, 1975

[7] Budai József: A kolera világjárványai, Lege Artis Medicinae, 15. évfolyam 2. szám/2005 pp. 8-9., ISSN 0866-4811

[8] Vedres István: Bacterialis és vírusfertőzések. Variola (himlő). pp. 540-545.. in Fodor Ferenc – Vedres István (szerk.) A közegészségtan és járványtan alapjai, második kiadás, Medicina Budapest, 1975

[9] World Health Organization WHO: Smallpox; http://www.who.int/mediacentre/factsheets/smallpox/en/; (2011. 04. 20.)

[10] Centers for Disease Controll and Prevention: History and Epidemiology of Global Smallpox Eradication; http://www.cdc.gov/search.do?queryText=smallpox+eradication&action=searchemergency.cdc.gov/agent/smallpox/training/overview/ppt/eradicationhistory.ppt; (2011. 04. 20.)

[11] Budai József Influenza, avián influenza – pandémia? HIPPOCRATESSM Családorvosi és foglalkozás-egészségügyi folyóirat, 2005. augusztus - szeptember - október VII.évfolyam 4. szám, pp: 238-241 ISSN 1419-3337

[12] Budai József, Influenza – madárinfluenza. Fenyeget-e pandémia? LAM Lege Artis Medicinae, 15. évfolyam 3. szám/2005. pp. 207-209., ISSN 0866-4811

[13] Ungchusak K, et al. Probable person-to-person transmission of avian influenza A (H5N1). N Eng J Med 2005; 352:3 pp. 33-40., ISSN 0028-4793

[14] Szalka A., Tóth E., Sinkovits B.: Az influenza pandémia bekövetkezési valószínségének statisztikai előrejelzése, IME VII. évfolyam 6. szám 2008. július pp. 36-40., ISSN 1588-6387

[15] WHO: Evolution of a pandemic A(H1N1) 2009 April 2009 – March 2010; http://whqlibdoc.who.int/publications/2010/9789241599924_eng.pdf; (2011. 10. 21.)

[16] Budai József: Járványok a történelemben I. HIPPOCRATES$_{SM}$ Családorvosi és foglalkozás-egészségügyi folyóirat, 2003. január - február V. évfolyam 1. szám pp. 39-41., ISSN 1419-3337

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Pápai Tibor
tibor.papai@gmail.com

STANDPOINTS OF THE ORGANISATION OF THE CARE OF THE SERIOUSLY INJURED PERSONS ON THE ROLE 3 LEVEL

Absztrakt/Abstract

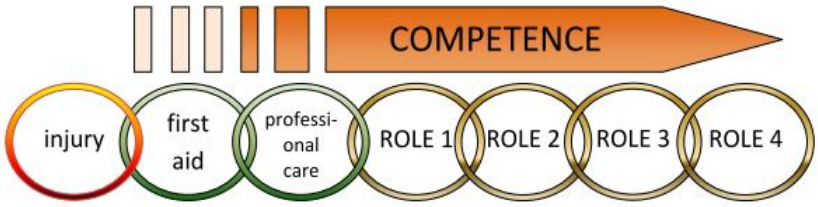
Magyar Honvédség Honvédkórház Sürgősségi Centrum összetett feladatrendszerében jelentős helyet foglal el a különböző sérültek magas szintű ellátása, szükség esetén a különböző katasztrófák sérültjeinek ellátása, valamint minősített időszakban a kórházi ROLE 3 szintű ellátás biztosítása. A súlyos sérült ellátása multidiszciplinális feladat, amely komoly szakmai kihívást jelent. A súlyos sérültek ellátása csak megfelelő humánerőforrás szervezéssel, képzéssel, hatékonyan működő triage rendszerrel, beteg utak menedzselésével, szakmai eljárás utasítások alkalmazásával biztosítható.

The high level care of the patients with different injuries, in need, the care of the persons injured in different catastrophes and in the qualified periods, the care of the inpatients on the ROLE 3 level take a significant place in the complex system of duties of the Military Hospital Emergency Center. The care of the seriously injured persons is a multi disciplinal duty that means a serious professional challenge. The care of the seriously injured persons can only be provided through the organisation, training of the suitable human resources, the effectively operating triage system, the management of the patient journeys, and the use of the professional procedure instructions.

Kulcsszavak/Keywords: *ROLE3, Honvédkórház, Sürgősségi Centrum, súlyos sérült, triage, algoritmus, képzés ~ ROLE 3, Military Hospital, Emergency Center, seriously injured persons, triage, algorithm, training*

1. THE DUTIES OF THE INTRAHOSPITAL EMERGENCY CARE

Nowadays, the system of the emergency care goes through significant changes – besides the priority of the care of the acute patients, the management of the patients with critical condition became emphasized better and better. The emergency medicine is a speciality that is dealing with the assessment, management, treatment and prevention of the diseases and injuries that cannot be planed and postponed. The duty of the emergency care units is to provide for a non-stop optimal health care with the suitable patient registration. Its target is that the patient arrives in the optimised condition, at an optimised time at the most optimised definitive place of health care. In the emergency health care system that operates after the concept of progression the Military Hospital Emergency Centre provides for a non-stop highest-level optimal health care with the suitable patient registration. The high level care of the patients with traumatology, combustive and neuro-traumatology injuries and, in need of the catastrophe care, the provision of these abilities take a significant place in the complex system of duties of the Centre. It is important to mention that the Military Hospital provides for the hospital (ROLE 3) and the rehabilitation (ROLE 4) duties both in the preventive protection and in the qualified periods. The main point of this is that during care on the front one has to follow the principles of the intermittent care of injured persons and those of the evacuation, whereas, every single injured soldiers has to be cared where it is needed according to the severity of the injury, then, the injured person has to be transported to the place of health care of higher level. Its first phase is the first aid on the front that is given by the soldiers for each other after the principle of fellow-soldier first aid when using their uniform field dressing. The second phase is the professional aid that is provided in a „nest for collecting the injured persons" that is formed not far from the front line, in a sheltered safe place for the injured soldier that received first aid on the front and who was transported there. A medical soldier with higher qualification and devices provides for the care of the injured persons here, until the injured person will be transported to the next level of health care. On the next levels, the injured person receives a professional care. They are the first dressing station (ROLE 1), then the first field hospital (ROLE 2), later the civil or military hospital care (ROLE 3) and, if needed, the hospital in the hinterland (ROLE 4). [1]



1. figure. The process of the care of the injured persons on the front

The medical officers and sub-officers regularly take part in the fulfilment of mission duties, in the course of which they perform the duties of different levels of the intermittent care of injured persons and those of the evacuation.

In each period, the Emergency Centre is forced to receive patients who are not forecasted, not classified and the number of who is not predictable and the condition and disease of whom are not defined exactly, moreover, the complexity and severity of their diseases are strongly variable. That is the reason why, the materials, personal and organizational conditions of the Emergency Centre that are necessary to the continuous and smooth operating have to be handled with emphasized attention and priority. In this case, I can declare that the Military Hospital Emergency Centre has the modern building construction that is necessary to its operation and the machines, instruments and devices of the

international level that are needed to a modern emergency care in the 21st century. The personal conditions are fulfilled according to the minimum conditions that are accepted by the professional board. Every single member of the crew has the knowledge, competence that is needed to the everyday emergency health care. We try to support the achievement and maintenance of these abilities and competences, beside the medium and high level qualifications accepted by the state, through regular trainings, practices and analyses of cases. During our work, we emphasize the pre-operative diagnose, the classification of the patients (triage), the development of the abilities and competences that are necessary to the care and nurse of the injured persons with different conditions. According to the present education system, our colleagues collect their basic qualification in the civil life, where they do not obtain any special, emergency, military, catastrophe health knowledge in the present education structure, that is the reason why their preparation for the special military, catastrophe emergency tasks, the determination and the development of the competences in connection with them mean a bigger challenge for us.

2. THE FEATURES OF THE CARE OF THE SERIOUSLY INJURED PERSONS

Within the tasks to be performed, the care of the seriously injured persons means a difficult professional, organizational and last but not least a significant financial challenge for us. The definition of a seriously injured / polytraumatised person can be stated in the real life only retrospectively that is the reason why we are forced to classify the severity of the injured person after the opinion of the person who gave the first aid. In the pre-hospital care one does not have any possibility for the refined diagnostics and the diagnosis of a polytrauma as defined can only be made after the examinations in the hospital, on the other hand, from the standpoint of emergency, the care of a seriously injured person and that of a poly-traumatised person happens according to the same scheme.

The care of a seriously injured person is a multi-disciplinal task, the survival of these persons can only be increased and the future quality of life of the injured person can only be improved by the close cooperation between the institutions and the care units. The trauma management based on ATLS means a priority in the care, this way, the approach that is focusing on time, the early operative stabilization (according to the principals of the damage control surgery), avoiding the development of the fatal trio (acidosis, hypothermia, coagulopathy). The period between the moment of the injury and the start of the definitive operative care means the gold watch that significantly determines the index of the success. Because of these standpoints, we lay a big emphasis on the development of the ability for the care of the seriously injured persons.

The care of the seriously injured persons caused by different accident mechanism can happen in times of peace during the everyday work, practices and under the special catastrophe or front conditions.

The injuries of different mechanisms that are developing in times of peace show an increasing tendency in our country too. The statistical figures show that the percentage of the occurrences of the accidents is very big, for the reason of which one can mention several factors (technical improvement, changes of the way of life etc.). As far as our country is concerned, people can seriously be injured in the classified situations with different size and even bigger frequency, such as catastrophe, high flood and we also have to calculate with special injuries caused by different explosions with industrial type, different remaining war constructions of detonation which were not defused or different acts of terrorism, underworld reckonings. People can also be seriously injured during the special exercising and training practices of the Hungarian Army (gunnery practices, chemical practices, field practices) that are carried out in times of peace. The proportion of death in times of peace caused by the

injuries runs to about 10% that refers mostly to the age groups 5-44 years. In 50% of the cases, people die on the spot, in 30 % during the first 24 hours of the care in hospital. In 50%, the reason for the early death is the injury of the central nervous system (head injury); in 30-50% the death is caused by exsanguinations (injury of the chest, abdomen, pelvis, and femurs). After the data of the special literature, the early death can be cut down by about 48% through interventions on the spot carried out in time (ensuring breathing passages, checking bleeding, care of the chest injury, replacing fluids lost, through "deshocking" the patient) and the well-organised care in hospital.

Because of the special tasks of the hospital with ROLE 3 level, to keep the efficiency of the care of the injured people on the front one must not disregard the main specialities of the warfare of the 21st century that significantly influences the development of the tactics of care. The most often injuries on the front, which have to be cared, are the gun-shot, burst injuries, combustive injuries caused by missiles, fragment of a bomb, injuries caused by cover in through building collapse, fall from the height and in the accident of a high-speed motor car, war vehicle. The main characters of the injuries occurring in the open country are: injuries of the soft tissues, open and splintered fracture of bone and the closed limb and head injuries. In case of injuries in closed places (building, motor car), soft traumas, closed limb fractures, head and vertebral fractures, pelvis fractures and the different forms of morphology and functional changes of the internal organs can appear because of the barotraumas, it means, the injuries caused by the overpressure. The combustive injuries caused by the hot and fire in case of an explosion and the toxic harms caused by the gas products make the procedure of aid and care for special. [2] The reasons of the death caused by these injuries can be the structural breakdown of the vital organs and limbs, the acute loss of blood and the shock developed as a consequence of them, the respiratory insufficiency caused by the respiratory occlusion and the tension pneumothorax. About 90% of death on the front happens before the injured person arrives at the place where the patient can be cared. The reason for death can be in the first 10 minutes the intense structural breakdown of the vital organ, organs, within 2-3 hours the intense loss of blood, within 4-12 hours the organic insufficiency caused by the shock. The data of the special literature confirm that the primer death on the front can be significantly reduced through the aid in time, the optimisation of the length of time of transporting the injured persons and the operation of places of first professional emergency aid, this way, the proportion of the seriously injured persons reaching the hospital alive is significantly better. To keep the optimal index of the success, it is essential to reduce the length of time between the injury and the first care, to increase the level of the first professional care and the emergency aid and to perform the emergency surgical interventions, in optimal case, within 1 hour but at least within 6 hours. Essays pointed out that the proportion of the avoidable and salvable death on the front could run to 35-37 %, 15% from which can only be realised through starting the professional fellow-soldier aid in time. [3]

The tactics of the care on the spot in times of peace and in the qualified periods can be different because of certain points of view (safety environment etc.) During the care on the spot, one has to focus on surveying the condition of the injured person and only performing the urgent interventions (ensuring the vital functions) in order to hinder the progression of the clinical picture, which means an emergency transport pressure for the people who provide the on site care, this way, certain interventions (intubations, replacement of fluids lost) may be left out in order to transport the injured person to hospital as soon as possible.

The procedure of the care of the seriously injured persons, in the phase of the care both on site and in hospital, must be a regulated process. The target of the regulation of the care is the development of the common way of thinking and the common language of people taking part in the care, laying a big emphasis on the importance of the teamwork. The algorithm of the

care of the seriously injured persons determines the details of the cooperation, the suitable levels of competence regarding the doctors, nurses and other assisting personnel. [4]

3. DETERMINATION OF THE CONDITION OF THE SERIOULY INJURED PERSON ON SITE

The patient can arrive at the Military Hospital Emergency Center on shore with a rescue car or by air with a helicopter. The Emergency Center usually faces a force of correction when the patient arrives because the interventions that were failed during the care on site have to be replaced. The direct Tetra radio connection between the Emergency Center and the rescue unit supports the preparation for the reception of the patient and the situations of correction, this way, and the rescue unit that transports the injured person to the hospital can provide some pieces of important information. The alert of the team who performs the care happens through the communication with the rescue unit and the use of the unified RTS (Revised Trauma Score) checklist after the completion of a so-called pre-hospital triage, which supports the maximum use of the time we have for the care of the patient.

point	GCS	RR -systolic (Hgmm)	Respiratory rate (/min)
4	15 - 13	> 90	10 - 29
3	12 - 9	89 - 76	> 29
2	8 - 6	75 - 50	9 - 6
1	5 - 4	49 - 1	5 - 1
0	3	0	0

1. table. RTS (Revised Trauma Score) checklist

With the help of the attached checklist, through using a system on points, people who provide the care on site can define the condition of the injured person after three parameters, the level of GCS (Glasgow Coma Scale, which defines the depth of the consciousness of the injured person, persons after a method of three reactions of the patient), the level of the systolic blood pressure and the respiratory rate per minute. The shift-leading head surgeon of the Emergency Center organises the care team to the reception place after the defined points, *12 stable injured, 11-8 instable injured, 7-0 in extremis injured.* Essentially, the gradual composition is suggested, the more seriously the person is injured the more members the care team will have and in case of several injured persons; the selection of several teams may also be needed. [5]

4. COMPOSITION OF THE TEAM THAT CARES THE SERIOUSLY INJURED PERSON

The leader of the team can be an emergency medical specialist or traumatologist or anaesthetist specialist who is experienced in the care of seriously injured persons, has ATLS qualification and takes part in the „deshocking" care of minimum 10-15 seriously injured persons a year (minimum in 5 cases as the leader of the team).

The obligatory members of the Trauma team are in all cases:

- the shift-leading head surgeon of the Emergency Center or the emergency/ anaesthetist specialist nominated by him
- traumatologist 1 or 2 persons
- emergency nurse (minimum 2 persons)
- administrator / dispatcher
- hospital porter /assistant

Further members of the Trauma team are: traumatologist, radiologist specialist, radiologist special assistant, abdominal surgeon, neurosurgeon, thoracic surgeon, burn surgeon and, if needed, dental surgeon, vein surgeon, urologist, oculist, laryngologist, gynaecologist, endoscopes specialist.

Often happens that specialists have to be initiated already in the „deshocking" care too. Beside the members of the team, the radiology, the blood transfusion, the operating room and the intensive care unit have to be notified about the arrival of the injured person, persons.

The call of the necessary team happens according to the condition of the injured person determined by the RTS (stable – instable – in exteremis) after the principle of gradation as follows:

	stable	**instable**	**in extremis**
RTS	12	11 - 8	7 - 0
Stage of shock	0 – I	II - III	IV
TEAM MEMBERS TO BE ALARMED			
emergency doctor	X	X	X
emergency nurse 1	X	X	X
emergency nurse 2	X	X	X
traumatologist 1	X	X	X
administrator	X	X	X
traumatologist 2	optional	X	X
anaesthesiologist	optional	X	X
anaesthesiologist assistant		optional	X
radiologist		X	X
abdominal surgeon		X	X
neurosurgeon		optional	X
thoracic surgeon		optional	X
hospital porter 1	X	X	X
hospital porter 2	X	X	X

2. table. Alarm plan for the care of seriously injured persons

5. STANDPOINTS OF THE RECEPTION OF AN INJURED PERSON

When receiving an injured person, in order to avoid the distortion of the information and to minimise the loss of information the leader of the transporting rescue unit informs the leader of the care team. The administrator or the leader of the transporting unit writes the most important pieces of information that were given during the verbal transfer (accidental mechanism, interventions performed on site, their duration and time, the ingested medicines, infusions, etc.) on the table mounted in the care room. The pieces of information on the table provide some help for the specialists who join the care team only later, its advantage is that the leader of the care team does not have to tell the pieces of information every time, this way, the care will be more orderly, cutting on the number of the failures that may occur during the care. Beside the verbal transfer of the information, the data that are needed to the care will be recorded and documented on the Case Report Form made regular by the Ambulance Service, then, we handle the copy of the Case Report Form as attached to the documents of the patient according to the valid regulations.

6. THE ELEMENTS OF THE FIRST EXAMINATION

Hereinafter, the elements of the first examination will be specified in the order of the priority of A-B-C-D-E algorithm (airway, breathing, circulation, disability, exposure) according to the emergency examination, however, this order is only theoretical because the main point of the regulated and well coordinated teamwork is to optimise the time of care the best as possible through performing certain tasks at the same time, if applicable, that is why the first examination has to be performed within 5 minutes, if possible. In order to keep the time interval, it is extraordinary important that everybody knows his task according to his competence and performs it with the possible biggest ability and discipline.

		Emergency doctor	Traumatologist 1 - 2	Emergency nurse 1	Emergency nurse 2	Administrator
Primary examination	A	oxygenation ensure.breath. passage medication anamnesis	analysis of the injury mechanism cervical immobilization in need: surgical breath passage	monitoring (SpO_2, HR, NIBP, B, T) EKG	implementing oxygen therapy, assistance by ensuring the breath passage	recording the data of the patient recording the anamnesis recording the care on-site recording the parameters, interventions requests for the laboratory examinations blood order request for different examinations (X-ray, CT, UH) notification of the conference of doctors dispatcher tasks
	B	respiration	chest detensialisation	respiratory toilet $EtCO_2$	assistance by the chest detensialisatio n	
	C	follow-up the dynamics of the vital-parameters venous in need: catheterisation (CV, IO) AVGA analysis	search and care the source of bleeding in need: order of a blood-stanching operation	peripheral catheterisation taking of blood central venous catheter, IBP measurement, preparation of AVGA	replacement of fluids lost in need: assistance by ensuring CV or IO catheter	
	D	GCS, examination of the pupils	examination of the cranium GCS, examination of the pupils	inserting an urinary catheter	in need: Inserting nasogastric tube	
	E	protection against hypothermia warming	examination of the dorsum	total undressing warming of the injured person	total undressing warming of the injured person	
Secondary examination		making a radiology and operative plan initiating partner specialists transfusion	detailed examination wound care fixing of fractures-dislocations AT/TETIG antibiotics	assistance by the wound care dosage of the ordered medicines	preparation of the transport	

***3*. table.** The course of the care of the seriously injured person, after competences

Conditions to be excluded and prevented during the first examination:

- blocked breath passage
- tensional PTX
- cardialis tamponade
- Life-threatening internal and external bleeding
- open pelvis
- hypothermia

At the end of the first examination, one has to consider whether the injured person has to be taken to further examinations or the operative care is needed immediately. The main principle of the decision has to be the dynamics of the parameters of the injured person. The further way of the injured person can go into two directions:

- prompt operative care
- ahead to the second examination (secondary survey)

Beside the machines, devices and medicines that are necessary to the emergency health care, the following special devices have to be available in good operable condition in the deshocking room.

- CT-MRI compatible rescue boat (spineboard) with the suitable head-neck fixer
- Pelvis fixer
- Limb puller-fixer
- Devices for the warming of the injured person
- Presence of the suitable trays, sets
  - Devices, medicines for ensuring the breath passage (carriage that is suitable for carrying out RSI)
  - Devices for the chest detensialisation
  - IO (intraosseous) needle
  - CV (central venous) set
  - DPL (diagnostic peritoneal lavage) set
- Fluid and blood-warmer
- US equipment (In case of an instable and in extermis injured person, for the preparation of FAST US)
- Blood preparations

7. THE ELEMENTS OF THE SECOND EXAMINATION

The first step of the preparation for the second examination is the full undressing of the injured person, in best case, it already happens in the ambulance car, if not, during the first examination it has to happen to the extent that is necessary for the examination and the intervention. As, 60% of the injured persons can be in hypothermic condition, during the care one has to monitor the temperature of the injured person and just in all cases one has to use heat preserving cover, if needed, the injured person has to be warmed actively. During the second examination, a detailed physical examination (from top to bottom) has to be performed in the deshocking room and to set up a further diagnostic plan with equipments. This can only be started, if the injured person is in relative stable condition, in case of an instable injured person one has to focus on the operation in order to stabilize the condition of the injured person as soon as possible.

8. THE ROLE OF THE COMMUNICATION AND THE EDUCATION IN THE CARE

The process of the care of the above-described seriously injured person reflects well that the management of the injured person requires a coordinated organisation and teamwork. The care of a seriously injured person means teamwork with the suitable leading and communication. The following points emphasize the suitable communication and the interaction between the members of the team; using this one can cut on the disorders of competence and communication that deteriorate the quality of care:

- Closed-circuit communication,
- Clear, explicit messages,
- Clear task for the team members,
- Confirming the fulfilment of the instructions,
- Summary and information sharing among the members,
- Respecting the team-mates,
- Knowing the own limits,
- Constructive intervention in case of a false decision.

Beside the communication, one has to lay a significant emphasis on the follow-up, development of the abilities of the participants with which we can guarantee the quality health care. From the viewpoint of the quality education one has to emphasize the development and follow-up of the knowledge of the teachers and the transfer of the new, both professional and methodological concepts and practices as soon as possible. That is the reason why we are organising practical trainings for the participants of the health care, on the basis of unified summary of lectures. Before the practical trainings, the participants have to learn the institutional protocols of the care of a seriously injured person. After learning the skills, the main purpose of the practices is to build them into the respective scenarios and to suitably adapt those in taking part in the care under the certain circumstances, with the real means.

9. SUMMARY

To sum it up, one can tell that the biggest enemy of the injuries, sudden health damage happened both in times of peace and in qualified situations is time. Through the early started, suitably organised care of the injured person, we can save life and we can save the injured person from the irreversible damage that influences the future quality of his life. The regulation of the course of the care and the suitable training and education of the professional staff taking part in the care is of emphasized importance in order to reach these targets.

References

[1] E. John Wipfler et all: Tactical Medicine Essentials Jones and Bartlett Publishers 2011. Canada

[2] Levente Várhelyi: Questions of the surgical care of the explosion injuries – Doctoral dissertation ZMNE (2010)

[3] Elsevier Mosby: Basic and Advanced Prehospital Trauma Life Support, Military edition, 2005

[4] Care of a seriously injured person in the Emergency Care Unit, The Professional Directive of the Ministry of Health Budapest 2010.

[5] Richard V. Aghababian: The grounds of the emergency medication, Medicina Könyvkiadó Zrt. Budapest, 2011

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Tamási Béla
tamasi.bela@hm.gov.hu

A HONVÉDELMI KATASZTRÓFAVÉDELMI RENDSZER MŰKÖDÉSÉNEK ELEMZÉSE NUKLEÁRIS BALESET ESETÉN

Absztrakt

Egy nukleáris vagy radiológiai veszélyhelyzet fenyegetést jelent, vagy jelenthet a lakosság egészségére, anyagi- és környezetbiztonságára. Magyarországon, kormányzati felelősség a bekövetkezett események megfelelő kezelése. Az események kezelése helyi, vagy területi szinten valósul meg, ami a veszély típusának, nagyságának és helyének függvényében az ország teljes területére kiterjeszthető. Magyarország, mint a Nemzetközi Atomenergia Ügynökség tagja természetesen felkérés esetén segítséget nyújt a más országokban bekövetkezett nukleáris veszélyhelyzet kezelésében. A Magyar Honvédség a hazai és a nemzetközi feladatban kijelölt erőkkel vesz részt. Ez a folyóiratcikk, a Magyar Honvédség nukleáris-baleset elhárítási tevékenységét foglalja össze.

A nuclear or radiological emergency is an emergency event that has led, or could lead, to a radiological threat to public health and safety, property, or the environment. In Hungary, every level of government has responsibility in the event of a nuclear or radiological emergency. Response begins at the local or municipal level, and progresses to the country level, depending upon the location, type, and size of the emergency. As a signatory country on the International Atomic Energy Agency (IAEA) convention, Hungary also has a responsibility to notify other countries if it has had a radio-nuclear incident, and to assist other countries with their own emergency response to a nuclear emergency if requested to do so. The Hungarian Home Defense Forces with its designated units has fundamental task in the emergency response. This article summaries those tasks.

Kulcsszavak: *nukleáris baleset, Magyar Honvédség, nukleáris erőmű, műhold, dominóhatás, tömegpusztító fegyverek ~ nuclear accidents, nuclear power plant, the Hungarian Army, satellite, domino effect, weapons of mass destruction*

1. BEVEZETÉS

Nukleáris erőmű hazánkban Pakson található, ezen túlmenően Budapesten egy tanreaktor valamint egy kísérleti kutatóreaktor is üzemel. Az országban több helyen találhatók kutatási és gyógyítási célokat biztosító izotóp laboratóriumok. A nukleáris anyagok, kiégett fűtőanyagok, izotópok szállítása mindennapi kockázatot rejt magában. Egy műhold-meghibásodás és annak visszajutása a Földre is potenciális veszélyforrás jelent a működéshez szükséges energiát biztosító nukleáris energiaforrás miatt. A tömegpusztító fegyverek alkalmazása ugyan be van tiltva, de szélsőséges csoportok, terroristák nyilván a nemzetközi megállapodásokat nem tartják be. A nukleáris katasztrófák minden esetben a dominóhatásnak megfelelően károsítják a környezetet, annak elemeit, így egyúttal biológiai katasztrófát is okoznak. Nem túlzás, ha azt mondjuk, hogy a radiológiai anyagok a ma emberének talán a legpotenciálisabb veszélyeztető tényezői. Az állampolgárok biztonságát a katasztrófavédelem részeként működő Országos Nukleáris-baleset Elhárítási Rendszer működtetésével valósítják meg. Ennek egyik erőssége a Magyar Honvédség erre a feladatra kijelölt egységei.

2. A HONVÉDELMI KATASZTRÓFAVÉDELMI RENDSZER KAPCSOLÓDÁSA AZ ORSZÁGOS NUKLEÁRIS- BALESETELHÁRÍTÁSI TEVÉKENYSÉGHEZ

A 89/2005. (V.5) Korm. rendelet mellékletei tartalmazzák a Nukleáris Biztonsági Szabályzatokat. A szabályzatokban található nukleáris-balesetelhárítási követelmények meghatározzák a nukleáris létesítmények baleset-elhárítási készültségét. *Az előírások jelentős mértékben a nemzetközi irodalomra, elsősorban a Nemzetközi Atomenergia Ügynökség dokumentumaira támaszkodnak, de emellett kapcsolódnak az Országos Baleset-elhárítási Intézkedési Terv (továbbiakban: OBEIT) definícióihoz, meghatározásaihoz is. Ezen túl a követelmények értelmezésére, az elvárt teljesítési mód meghatározására az Országos Atomenergia Hivatal főigazgatója hatósági útmutatót bocsátott ki. A szabályzatok és az útmutató követelményei egységes elvárás/ajánlás rendszert képeznek a nukleáris létesítmények baleset-elhárítási felkészülésével szemben.*[1]

A Honvédelmi Katasztrófavédelmi Rendszer *(továbbiakban: HKR)* a katasztrófák elleni védekezésről szóló jogszabályok[1]alapján működik, ezen belül illeszkedik Országos Nukleárisbaleset-elhárítási Rendszerhez *(továbbiakban: ONER)* és ennél fogva természetesen a rendszer egyik eleme. *A HKR vezető szervei, illetve a rendszerbe kijelölt erők minden katasztrófatípus esetén rögzített feladatrendnek megfelelően működnek. Nukleáris esemény bekövetkezése esetén a HKR kijelölt erői közül az adott katasztrófatípus elhárítására leginkább igénybe vehető munkacsoportok részvétele várható. A nukleárisbaleset-elhárítási feladatok végrehajtására elsősorban vegyi-védelmi és műszaki, továbbá más szakterületi ismeretekkel rendelkező, nukleárisbaleset-elhárítási ismeretekből felkészített, egyéni védőeszközökkel felszerelt személyi állomány kerül alkalmazásra.*[2]

Az OBEIT-ben, a Magyar Honvédség *(továbbiakban: MH)* részére meghatározott nukleárisbaleset-elhárítási szakfeladatokat jellemzően az alábbi munkacsoportok állománya hajtja végre:

- Atom-, biológiai és vegyi felderítő csoport;
- Atom-, biológiai és vegyi mentesítő csoport;
- Légi sugárfelderítő csoport;
- HAVARIA laboratórium;
- Ágazati Információs Központ;
- Légi sugárfelderítő tiszti járőr;

[1] Lásd a felhasznált jogszabályok jegyzékében

- Sugár-egészségügyi laboratórium
- Orvosi ellátó csoport és a biztosított kórházi ágykapacitás;
- Mobil orvos csoport;
- Nehéz földmunkagép és gépi romeltakarító csoport;
- Vízi szállítócsoport. [3]

Nukleáris baleset bekövetkezése esetén, a fenti munkacsoportokon kívül a HKR bármely munkacsoportja kirendelhető, de kizárólag a rendeltetésének megfelelő katasztrófavédelmi feladatokra, amennyiben a biztonságos munkavégzés egyéb feltételei (kiemelten a sugárvédelem) biztosítottak.

3. A HKR VEZETŐI, SZERVEI ÉS A VÉGREHAJTÓ ERŐK FELELŐSSÉGE NUKLEÁRIS VESZÉLYHELYZETBEN

A *honvédelmi miniszter* felelős az MH feladatkörébe tartozó nukleárisbaleset-elhárítással kapcsolatos tervező, szervező és irányító tevékenységért. Ennek keretében rendelkezik a veszélyhelyzeti intézkedések ágazaton belüli érvényesülésének szabályairól, és előterjeszti a kormány részére a HKR nemzetközi nukleárisbaleset-elhárítási segítségnyújtásban közreműködő erők és eszközök kijelölésére, felhasználására vonatkozó javaslatot. A nukleárisbaleset-elhárítás időszakában dönt az erők kirendeléséről és a 3000 főt meghaladó kirendelés esetén, tájékoztatja az Országgyűlést.

A *Honvédelmi Minisztérium közigazgatási államtitkár (továbbiakban: HM KÁT)* a Kormányzati Koordinációs Bizottság *(továbbiakban: KKB)* tagjaként képviseli a honvédelmi tárcát a KKB ülésein, és a Honvéd Vezérkar főnök vezetői tevékenységével irányítja a Katasztrófavédelmi Operatív Bizottságot *(továbbiakban: KOB)*. Feladata jóváhagyásra előterjeszteni a honvédelmi miniszter részére a nukleárisbaleset következtében kihirdetett veszélyhelyzet, illetve szükségállapot esetén alkalmazandó rendeleti úton bevezetett intézkedések ágazaton belüli érvényesülésének szabályait, valamint a minősített helyzetek kihirdetését el nem érő nukleárisbaleset esetén bevezetendő rendszabályokat. Továbbiakban koordinálja a nemzetközi nukleárisbaleset-elhárítási segítségnyújtásban történő ágazati részvételt, végzi a kormánydöntés előkészítési feladatait a KKB döntése alapján és felterjeszti a honvédelmi miniszternek a Honvéd Vezérkar főnökének jogkörét meghaladó kirendelésekre vonatkozó javaslatokat, előkészíti a tájékoztatót az Országgyűlés részére.

A *Honvéd Vezérkar főnöke (továbbiakban: HVKF)* tanácskozási joggal részt vesz a KKB munkájában, dönt a hatáskörébe tartozó erők kirendeléséről, irányítja a KOB tevékenységét és felügyeli az alárendeltségébe tartozó, nukleárisbaleset-elhárítási feladatokat végrehajtó állomány tevékenységét.

A *Honvédelmi Ágazati Katasztrófavédelmi Operatív Törzs (továbbiakban: HÁKOT)* kidolgozza a honvédelmi miniszter KKB tagságából a honvédelmi ágazatra háruló feladatok végrehajtásához szükséges előterjesztéseket, előkészíti a honvédelmi miniszter és a HM KÁT döntéseit és az általa meghatározottak szerint, koordinálja a feladatok végrehajtását. A HM Védelmi Hivatal (továbbiakban: HM VH) főigazgatója útján folyamatos kapcsolatot tart fenn a védekezésben érintett minisztériumok, országos hatáskörű szervek, a védelmi igazgatás területi és helyi szerveinek, valamint a honvédelemben közreműködő szervek vezetőivel, elemzi az információkat, és végzi a szükséges koordinációt, közreműködik a fővárosi és megyei védelmi bizottságok hatáskörébe utalt döntések előkészítésében és végrehajtásában.

A *Katasztrófavédelmi Operatív Bizottság (továbbiakban: KOB)* riasztja a nukleárisbaleset-elhárításra kijelölt honvédségi erőket, kezdeményezi azok igénybevételét. A HVKF, illetve a honvédelmi miniszter döntése alapján kirendeli a riasztott erőket, kapcsolatot tart fenn, illetve együttműködik az érintett ágazatok baleset-elhárítási szervezeteivel. Irányítja a nukleárisbaleset-elhárítási feladatok végrehajtásába bevont erőket és a nukleáris baleset

következményei által veszélyeztetett katonai szervezetek állományának megóvására irányuló feladatokat. Végrehajtja a várható és a bekövetkezett katasztrófák felméréséhez, értékeléséhez szükséges információk gyűjtését és feldolgozását, az adatközlést (adatcserét), valamint javaslatot tesz a nukleárisbaleset-elhárításba bevonandó további MH erők kijelölésére, felkészítésére.

A KOB irányítási feladatait a kialakult helyzet függvényében a Katasztrófa Operatív Csoportok, az összekötők, valamint az MH Központi Ügyelet és a hadműveleti ügyeleti szolgálatok útján valósítja meg.

A *Katasztrófavédelmi Operatív Csoportok (továbbiakban: KOCS)* a KOB irányítása alapján, a saját Katasztrófa Alkalmazási Tervekben *(továbbiakban: KAT)* és az Ágazati Katasztrófavédelmi Tervben *(továbbiakban: ÁKT)* meghatározott rendben megfelelően vezetik az alárendelt végrehajtó erők nukleárisbaleset-elhárítási tevékenységét.

Az *Ágazati Információs Központ (továbbiakban: ÁIK)* feladata a nukleáris, vegyi és biológiai veszély előrejelzésére, felmérésére ellenőrző és jelző szervezet működtetése, folyamatos mérési adatok szolgáltatása a Magyarország területén a gamma-háttérsugárzás szintjéről, helyi és központi riasztás kezdeményezése vegyi, nukleáris vagy biológiai veszély jelenléte esetén. A beérkezett információk, valamint az adatbázisok felhasználásával a nukleáris, vegyi és biológiai helyzet előrejelzése, az előrejelzés alapján javaslat felterjesztése a veszélyeztetett területen katasztrófavédelmi feladatot végrehajtó szervezetek tevékenységére, javaslat készítése a valós veszélyes terület felmérésére. További feladata az adatszolgáltatás a nukleáris, vegyi és biológiai katasztrófák kezeléséhez, valamint meteorológiai és egészségügyi információk nyújtása a KOB döntéseinek előkészítésére és a döntések alátámasztására.

Az ÁIK felderítési igénye alapján végzi feladatait a légi sugárfelderítő csoport, aki a felderítési adatokat azonnal és változatlan formában jelenti a központnak az MH Vegyi-Sugárfigyelő Helyzetértékelő Ügyeleti szolgálaton *(továbbiakban: MH VSFHÉÜSZ)* keresztül. Ugyanígy valósul meg az atom-, biológiai-, vegyi felderítő csoport által szolgáltatott felderítési adatok, a HAVARIA laboratórium és az AMAR[2]támogató csoport jelentése is. [4]

A védekezés időszakában a feladatok végrehajtása az alábbi dokumentumok alapján történik:

- az OBEIT-tel összhangban álló ÁKT;
- a KOCS-ok megalakítására kötelezett szervezetek által elkészített KAT-ok;
- a katonai szervezetek belső- és külső védelmi tervei;
- a megyei (fővárosi) védelmi bizottságok által a nukleárisbaleset-elhárításra kidolgozott baleset- elhárítási intézkedési tervek.

A nukleárisbaleset-elhárítási feladatok végrehajtásában csak a kijelölt és felkészített, munkavédelmi vizsgával rendelkező, a szükséges egyéni védőeszközökkel, egészségvédelmi felszereléssel ellátott erők vesznek részt. A katasztrófavédelmi tevékenységet végző katonai erők sem polgári, sem más szerv alárendeltségébe nem kerülnek, irányításuk a HKR vezetési rendje szerint történik. A katasztrófavédelmi munkák helyszínén szakmai feladataikat a helyi védelem irányítását végző vezető határozza meg, a kirendelt honvédségi erők parancsnokai útján.

[2] Automata Mérő és Adatszolgáltató Rendszer

4. A RIASZTÁS ÉS AKTIVIZÁLÁS RENDJE NUKLEÁRIS ESEMÉNY BEKÖVETKEZÉSE ESETÉN

A HÁKOT állandó tagjai, a KOB és a KOCS-ok kijelölt állománya, a KKB Operatív Törzsébe és a KKB Védekezési Munkabizottságba kijelölt szakértők, valamint a végrehajtásra kijelölt erők meghatározott elemei lakáson eltöltött készenléti szolgálatot látnak el. A MH Központi Ügyelet *(továbbiakban: MH KÜ)* folyamatosan kapcsolatban áll a KKB Veszélyhelyzeti Központ Ügyelettel. A honvédségi erők katasztrófavédelmi célból történő kirendelésének általános rendje szerint az igényre vonatkozó kérést a KKB-hoz (vagy a KKB Operatív Törzséhez) kell felterjeszteni. A KKB (vagy a KKB Operatív Törzse) az igényeket továbbítja az MH KÜ-nek.

Ha a KKB-t nem hívják össze, az igénybevételre vonatkozó kérést a BM Országos Katasztrófavédelmi Főigazgatóság *(továbbiakban: BM OKF)* bázisán működő Veszélyhelyzeti Központ közvetlenül az MH KÜ részére küldi meg. A kirendelésről a honvédelmi miniszter, illetve a HVKF dönt. A kirendelésre vonatkozó igényt a kezdeményezőnek – a felkészülés érdekében – a KKB-hez történő felterjesztéssel egyidejűleg az MH KÜ-nek is meg kell küldenie. Az MH KÜ az igénylést továbbítja a KOB ügyeletes vezetőjének, illetve a részére meghatározott személyeknek, szervezeteknek. (HM KT, HM VH stb.) Rendkívüli esetben, a veszélyeztető nukleáris létesítménytől, vagy a területileg illetékes megyei (helyi) védelmi bizottságtól, az MH VSFHÉÜSZ-től, vagy más szervtől kapott hiteles riasztás-értesítés alapján, amennyiben a HKR nincs aktivizálva és az állomány testi épségének megőrzése indokolja az azonnali intézkedést, a nukleárisbaleset által érintett katonai szervezet parancsnoka saját hatáskörében dönt az alárendeltségébe tartozó állomány által foganatosítandó óvintézkedésekről.

Nukleáris baleset bekövetkeztése esetén a HKR riasztása jellemzően az alábbiak szerint történik:

- a BM OKF főügyeletének értesítése,
- az MH Vegyi-, Sugárfigyelő, Helyzetértékelő Ügyeleti Szolgálat (továbbiakban: VSFHÉÜSZ) értesítése alapján, az MH KÜ-n keresztül.

A KKB-től vagy annak szerveitől érkező, katasztrófavédelmi feladatokhoz való hozzájárulásra történő felkérés esetén a HKR egésze vagy elemei katasztrófavédelmi riasztására (aktivizálására, katasztrófavédelmi készenlétbe helyezésére) a HM VH főigazgató, a HM Tervezési és Koordinációs Főosztály főosztályvezető, valamint az MH Vezetési és Doktrinális Központ parancsnok közös javaslata alapján a HM KÁT jogosult. A felső és középszintű katasztrófavédelmi vezetőszervek katasztrófavédelmi riasztását, aktivizálását – halasztást nem tűrő esetben a HM KÁT egyidejű tájékoztatása mellett – a KOB vezetője is jogosult elrendelni.

5. A HONVÉDELMI TÁRCA FELADATAI A NUKLEÁRISBALESET-ELHÁRÍTÁSI FELADATOKRA VALÓ FELKÉSZÜLÉS ÉS A MEGELŐZÉS IDŐSZAKÁBAN

A felkészülés és megelőzés időszakának ágazati feladatai az alábbiak:

- *katasztrófavédelmi felkészítés folytatása* a HKR-be kijelölt erők, illetve az MH teljes személyi állománya részére a vonatkozó mértékben;
- *a végrehajtó erők munkacsoportjainak gyakoroltatása, részvétel az ágazati, országos és nemzetközi nukleárisbaleset-elhárítási gyakorlatokon;*
- a HKR-be kijelölt erők és eszközök folyamatos alkalmazhatóságának biztosítása;
- *nukleáris baleset által veszélyeztetett* katonai szervezetek *állományának védelmére irányuló, illetve a nukleárisbaleset-elhárításban részt vevő erők alkalmazását biztosító rendszabályok, tervek kidolgozása.*[5]

A nukleáris balesetre való felkészülés keretében a honvédelmi ágazat fő felelőssége a saját állományának megóvása. Az ONER-ben az MH speciális képességei igénybevételével közreműködik a nukleárisbaleset-elhárítási feladatok ellátásában.

A felkészülési és a megelőzés időszak tervezése központilag a HM és az MH éves (havi) feladattervezési rendszerén, valamint a katasztrófavédelmi költségtervezés rendszerén keresztül, továbbá a kiképzési, felkészítési, illetve rendezvénytervek útján valósul meg.

A képzés és gyakoroltatás felelőssége, módja, résztvevői:

A HM KÁT: irányítja a KOB katasztrófavédelmi felkészítését, kiképzését, továbbképzését, a HKR elemeinek gyakorlatokon történő részvételét.

A HVKF:

- intézkedik a katasztrófavédelemre kijelölt állomány felkészítési rendszere, módszere, tematikája kidolgozására;
- irányítja a középszintű vezetőszervek katasztrófavédelmi felkészítését, kiképzését és a gyakorlatok tervezését;
- biztosítja az országos katasztrófavédelmi rendszer, nemzetközi együttműködés keretében szervezetett közös kiképzéseken; gyakorlatokon történő részvételét.

A KOB vezetője: a HM államtitkárnak jóváhagyásra felterjeszti a KOB felkészítési tervét.

Az állományilletékes parancsnok: végrehajtja az érintett állomány kiképzését, és a védelmi tervben meghatározott feladatok begyakorlását.

A Nemzeti Közszolgálati Egyetem és az MH Altiszti Akadémia

- az alapképzésében oktatja a katasztrófavédelemi ismereteket;
- az MH igénye szerint megszervezi a tanfolyamrendszerű katasztrófavédelmi képzést.

A HKR a nukleárisbaleset-elhárításra történő felkészülés és megelőzés időszakában nincs aktivizálva, az abba kijelölt szervezetek a „honvédelmi ágazat katasztrófák elleni védekezésének irányításáról és feladatairól” szóló 23/2005. (VI. 16.) HM rendelet alapján végzik tevékenységüket, biztosítják a működési feltételeket. Az elsődleges beavatkozásra tervezett erők speciális munkacsoportokba szervezve, lakáson ellátandó készenléti szolgálatot látnak oly módon, hogy riasztásuk esetén feladataik megkezdésére a riasztást követő 6. órában készen álljanak.

A HKR mérő, ellenőrző és jelző szervezetének nukleárisbaleset-elhárítási feladatait az MH Atom, Vegyi, Biológiai Riasztási és Értesítési Rendszer (továbbiakban: ABV RIÉR) kijelölt elemei végzik. *Az MH ABV RIÉR az Országos Sugárfigyelő, Jelző és Ellenőrző rendszer (továbbiakban: OSJER) részeként, azzal összhangban hajtja végre feladatát. Normál időszakban is folyamatos mérési adatokat szolgáltat a Magyarország területén a gamma-háttérsugárzás szintjéről, helyi és központi riasztást kezdeményez nukleáris veszély jelenléte esetén.* [6]

Az MH ABV RIÉR (AMAR, a HAVARIA laboratórium és az MH Görgei Artúr Vegyivédelmi Információs Központ bázisán kialakított ÁIK) végzi normál időszakban az MH katonai szervezetei érdekében a valóságos sugárhelyzet felmérését, arról alapadatok szolgáltatását, a katonai felső vezetés napi tájékoztatását, biztosítja a készültségi fokozatokba helyezés feltételeinek fenntartását.

6. A HKR MŰKÖDÉSE A NUKLEÁRIS VESZÉLYHELYZET KÜLÖNBÖZŐ IDŐSZAKAIBAN

6.1. A készenléti működés során

Az ONER készenléti működési állapotának meghatározását és az MH kijelölt erőinek érintettségének megállapítását követően a honvédelmi tárca értesítése, a kijelölt erők riasztása a HKR készenléti rendszerében, a hatályos jogszabályoknak, intézkedéseknek és terveknek megfelelően történik. Az ONER készenléti működésének elrendelése esetén jellemzően a honvédelmi ágazat által működtetett mérőrendszer fokozott működésével, a HKR vezető szervei részleges vagy teljes aktivizálásával, a katonai felső-vezetés és az együttműködők gyakori és részletes tájékoztatásával kell számolni. A nukleárisbaleset-elhárításra kijelölt speciális készenlétű munkacsoportok munkahelyi készenlétének elrendelése, szakfeladatok ellátására történő felkészülésük a kialakult konkrét helyzet függvényében szükségessé válhat. Ekkor a személyi állomány megóvása érdekében rendszabályok bevezetése nem várható.

A HKR szervezeteinek várható szakfeladatai az ONER készenléti működése során.

- Az ÁIK aktivizálása és áttérése váltásos munkarendre;
- A HAVARIA laboratórium felkészülése, szükség esetén mintavételi és azonosítási tevékenység végzése;
- Az AMAR támogató csoport felkészülése és szükség esetén mobil AMAR állomások telepítése;
- A légi sugárfelderítő csoport aktivizálása és szükség esetén szakfeladat végrehajtása.

6.2. Működés a nukleáris veszélyhelyzet korai időszakában

A honvédelmi ágazatnak a sürgős óvintézkedési tevékenysége és felelőssége a nukleárisbaleset következtében veszélyeztetett saját csapatok kimenekítése a külső védelmi tervekben meghatározottak szerint. Nukleárisbaleset-elhárítás során a HKR kijelölt erői a KKB és a NVM felkérése alapján közvetlenül részt vesznek a Paksi Atomerőműben bekövetkezett baleset elhárításában, illetve közreműködnek az egyéb nukleáris veszélyhelyzet hazai következményei elhárításában.

Az MH konkrét tevékenysége:

- részvétel a Paksi Atomerőmű 30 km-es sugarú körzetének földi és légi sugárfelderítésében, a sugárzási viszonyok változásának folyamatos ellenőrzésében;
- részvétel a nukleáris veszélyhelyzet felszámolásába bevont polgári erők sugármentesítésében;
- részvétel a sérültek első orvosi, illetve kórházi ellátásában;
- szükség esetén kompátkelőhelyek berendezése, utak helyreállítása;
- a Sugárfigyelő Rendszer saját állomásainak üzemeltetése.

A kijelölt erőktől elvárt teljesítőképesség:

- Légi sugárfelderítés, max. 600 km^2/óra;
- Földi sugárfelderítés, max. 250 km^2/óra;
- Mentesítés, 70 gépjármű/nap;
- Fürdetés ,100 fő/óra.

A HKR nukleárisbaleset-elhárításra kijelölt erőinek a helyettesítésére, pótlására a sugárszint függvényében első fokon a kijelölt erőket biztosító (vegyivédelmi, műszaki stb.) katonai szervezetek állományából kerül sor. A helyettesítésre, pótlásra másodfokon az MH további katonai szervezeteinek a megfelelő szakképesítésű (vegyivédelmi, műszaki stb.) állományából kerülhet sor. Amennyiben a HKR végrehajtó erői elégtelennek mutatkoznak a katasztrófavédelmi feladatok ellátásához, megfelelő felkészítés, illetve kiképzés után, további

erőket is be lehet vonni a tevékenységbe. A további erők kirendelésével kapcsolatos előírások a 23/2005 (VI. 16.) HM rendeletben vannak rögzítve. [7]

Az MH ABV RIÉR nukleáris veszélyhelyzetben végzi a KKB követelményei alapján az adatszolgáltatást a Magyarország területén kialakult vegyi-, sugárhelyzetről, az MH érdekében a valóságos vegyi, biológiai és sugárhelyzet gyors felmérését, az érintett szervek tájékoztatását, a veszélyeztetett katonai szervezetek gyors (közvetlen) riasztását.

Az MH ABV RIÉR részeként állandóan működtetett AMAR kiegészülhet a HAVARIA laboratóriummal, légi, és földi sugárfelderítő erőkkel, melyek alkalmazásával a valós sugárhelyzet felmérése megtörténik. A rendszer további laboratóriumi hátterét alkotják az MH Honvédkórház stacioner laboratóriumai.

A nukleáris veszélyhelyzet korai időszakában az ÁIK aktivizálásra kerül és váltásos munkarendben működik. Folyamatosan tájékoztatja a KOB-ot, a honvédelmi felsővezetést és az együttműködő ÁIK-okat a valós és várható sugárhelyzetről. Az ÁIK szakmai információkat nyújt a szaktevékenységekkel kapcsolatban, valamint javaslatokat tesz a foganatosítandó biztonsági rendszabályokra, a felderítési, mentesítési és egyéb felszámolási munkálatokra.

Az MH Összhaderőnemi Parancsnokság ABV Központja váltásos munkarendben működik, és folyamatosan támogatja a parancsnokság bázisán megalakuló KOCS-ot, jelenti a sugárhelyzetre vonatkozó felderítési adatokat az ÁIK-nak. A légi sugárfelderítő csoport végrehajtja a sugárhelyzet felderítését, kihullás esetén legkorábban a kihullás vége után 2 órával. A HAVARIA laboratórium meghatározott körzetekben és objektumok környezetében mintavételi és azonosítási tevékenységet végez. Az AMAR támogató csoport mobil AMAR állomásokat telepít a várható vagy a valós sugárhelyzet monitorozása érdekében.

Az ABV RIÉR nukleárisbaleset-elhárítással kapcsolatos adataihoz hozzáférhetnek:

- a KOB, valamint a KOCS-ok;
- az MH VSFHÉÜSZ, a szervizcsoport és az értékelő szervezet valamennyi állomása és az együttműködő ágazatok vonatkozásában teljes terjedelemben. A katonai szervezet saját mérési adataihoz, teljes terjedelemben, olvasási joggal,
- az elöljáró szervezetek a mérési eredményekhez saját alárendeltjeik vonatkozásában, olvasási joggal;
- a NATO hadszíntér-parancsnokság, a szomszéd tagországok értékelő szervezetei az általuk igényelt gyakorisággal;
- a KKB érintett szervei;
- a Nukleárisbaleset-elhárítási Védekezési Munkabizottság;
- az Országos Atomenergia Hivatal Baleset-elhárítási Szervezet;
- az KKB Veszélyhelyzeti Központ;
- a BM OKF Nukleáris Baleseti Információs és Értékelő Központ;
- az Országos Környezeti Sugárvédelmi Ellenőrző Rendszer Információs Központ az OSJER és más ágazatok a vonatkozó mértékben.

6.3. Működés a nukleáris veszélyhelyzet kései időszakában

Az ÁIK folyamatosan működik és tájékoztatja a HKR vezető szerveit és az együttműködő ÁIK-okat a valós sugárhelyzet változásáról. Javaslatokat tesz a foganatosított biztonsági rendszabályok enyhítésére, vagy további rendszabályokra, valamint a monitorozási, mentesítési és egyéb felszámolási munkálatokra.

Az MH Összahaderőnemi parancsnokság ABV Központja váltásos munkarendben működik és folyamatosan támogatja a parancsnokság bázisán működő KOCS-ot, jelenti a sugárhelyzetre vonatkozó felderítési adatokat az ÁIK-nak. A légi sugárfelderítő csoport a továbbiakban készenlétben marad és szükség esetén végez felderítést a sugárhelyzet pontosítása érdekében.

A HAVARIA laboratórium meghatározott körzetekben és objektumok környezetében mintavételi és azonosítási tevékenységet végez. Az AMAR támogató csoport mobil AMAR állomásokat üzemeltet a sugárhelyzet folyamatos monitorozása érdekében.

A helyi lakosság, az érintett helyszínen ideiglenesen tartózkodók, a speciális létesítmények áttelepítési feladataiban a HKR csak konkrét felkérés és a kialakult helyzet értékeléséből adódó döntést követően tud részt venni a rendelkezésére álló kapacitással. A kitelepített lakosság monitorozásában és sugár-mentesítési feladatokban, továbbá a sugárvédelmi támogató személyzet és felszerelés biztosításában a HKR csak segítségnyújtóként vesz részt.

A szennyezett sérülteknek nyújtandó, veszélyhelyzeti orvosi kezelésben a HKR 100 ágy mértékű kórházi kapacitással képes részt venni.

A fentieken felül jelentkező következmény felszámolási feladatainak a végrehajtásában csak a konkrét helyzetben történő felkérés után, bevont erők igénybevételével képes a HKR részt venni.

6.4. A honvédelmi tárca feladatai a helyreállítás időszakában

A honvédelmi ágazaton belül a helyreállítás időszakában végzendő feladatokról, hosszú távú intézkedésekről a kialakult helyzet függvényében történik döntés.

6.5. A lakossági és médiatájékoztatás rendje

A lakosságtájékoztatási, társadalmi kapcsolati és sajtóval való kapcsolattartási feladatok úgy a felkészülés-megelőzés, mind a védekezés időszakában kizárólag a HKR és a honvédelmi tárca nukleárisbaleset-elhárítási feladatainak megismertetésére irányulnak. Lakosságképzési feladata a honvédelmi ágazatnak nincs.

7. A RENDSZER TOVÁBBFEJLESZTÉSE ÉRDEKÉBEN TETT JAVASLATOK

Az előzőekben bemutatott feladatrendszerben hatékonyság csak akkor érhető el, ha a hivatásos katasztrófavédelem az állami szervek, más szakmai szervezetek, a gazdasági élet sok más szereplője és a társadalom, együtt, közösen vesz részt a katasztrófák elleni védekezésben, mind a megelőző felkészülési, mind a kárhatások felszámolási, mind a rehabilitációs időszakban.

A létszámában, (hadi)technikai eszközeiben racionalizált honvédségben, a HKR tevékenységének biztosítása érdekében az alábbi időszerű feladatok végrehajtását fogalmazom meg:

- Az MH-nak alkalmasnak kell lennie az új katasztrófavédelmi törvényben megfogalmazott feladatok zökkenőmentes ellátására, ehhez a HKR törvényi szabályzóit át kell alakítani, azonban az átalakítás nem eredményezheti a meglévő képességek akár időleges visszaesését sem;
- A katasztrófavédelmi tevékenységnek mindenben illeszkednie kell az ország katasztrófavédelmi rendszerének egészéhez, biztosítani kell a kapcsolódási pontokat a vezetési és a végrehajtó szinten egyaránt;
- Mivel mindeddig nem történt meg, a HKR rendszerének igazodnia kell a nemzetközi, elsősorban a NATO válságreagálási rendszeréhez (NCRS)[3], az ott alkalmazott eljárásokat a lehetőségek függvényében maximálisan adaptálni kell és meg kell határozni az ezzel kapcsolatos további feladatokat;
- A HKR felépítésének továbbra is hasonlónak kell lennie más ágazatok katasztrófavédelmi rendszeréhez, mivel ez biztosítja a személyi állomány

[3] NATO Crisis Response System

átjárhatóságát, szükség esetén más ágazatok szakembereinek gyors átvételét és alkalmazását;

- Fontos szem előtt tartani, hogy a kialakított szervezeti struktúrának és vezetési rendszernek csak a lehető legkisebb mértékben szabad eltérni a békében egyébként fennálló katonai szervezetek felépítésétől és a szolgálati hierarchiától;
- A mindenkor kialakított vezetési rendszernek a felső szinten is meg kell felelnie a Honvédelmi Minisztérium, illetve a Magyar Honvédség felső szintű vezetési rendszerének. A minisztériumi szinten a feladatokat a főosztályok és csoportfőnökségek bevonásával kell végezni;
- Meg kell határozni azt a szintet, amikor a Magyar Honvédség békeerőinek igénybevétele előreláthatólag már nem elegendő a katasztrófahelyzet kezelésére és nemzetközi segítség kérése elengedhetetlen;
- Tervszerűen, időszakonként ki kell kérni más minisztériumok és országos hatáskörű szervek szakembereinek véleményét, széles körű szakmai és közigazgatási egyeztetést kell lefolytatni a kérdésben;
- A felhasználásra tervezett eszközöknek korszerűnek és biztonságosnak kell lenniük, melyek kezelésére, használatára az állományt ki kell képezni. Az állomány katasztrófavédelmi területen szerzett képességeit a kiképzés során és gyakorlatok keretében rendszeresen ellenőrizni kell;
- Az Önkéntes Tartalékos Rendszerben rejlő lehetőségeket maximálisan ki kell használni;
- A HKR riasztása során a Magyar Honvédség riasztási rendszerét kell igénybe venni, melynek technikai feltételei, kiépítettsége és megbízhatósága adott;
- Biztosítani kell a katasztrófavédelmi rendszer működésével kapcsolatos időbeni tájékoztatás megszervezését és a társadalmi kapcsolatok folyamatos fenntartását.

8. BEFEJEZÉS

Minden nemzet alapvető kötelessége, egyben kormányzati feladat, megfelelő hatékonysággal kezelni a nukleáris energia használatából esetlegesen bekövetkező eseményeket. Így van ez hazánk esetében is. A katasztrófavédelem részeként működő Országos Nukleáris-baleset Elhárítási Rendszer feladata a bekövetkezett események káros hatásának csökkentése, a lakosság védelme. A Magyar Honvédség kijelölt erőivel vesz részt a feladatban. A vezetéstől a feladat végrehajtásig szigorú előírások határozzák meg a hatékony feladat végrehajtást. A cikk bemutatja a Magyar Honvédség közreműködését az Országos Nukleáris-baleset Elhárítási Rendszerben. A hazai nukleáris baleset-elhárítás rendszere az új katasztrófa törvény hatásait tekintve jelentősen nem változott. Ennek ellenére a rendszer folyamatos fejlesztése elengedhetetlenül szükséges. Az időszerű feladatok megfogalmazásával a fejlesztés irányaira tettem javaslatot, ami a Magyar Honvédség valamennyi katasztrófatevékenységére általános érvényű lehet . A rendszer hatékonyságát ellenőrzések, gyakorlatok keretében mérik. Remélhetőleg „éles” tesztelésre soha nem kerül sor.

Felhasznált irodalom

[1] Petőfi Gábor - Dr. Rónaky József - Solymosi József: A NUKLEÁRISBALESET-ELHÁRÍTÁSI KÖVETELMÉNYEK FEJLŐDÉSE; Hadmérnök II. évfolyam 1. szám, 2007. március p.58 ISSN: 1788-1919

[2] HONVÉDELMI KATASZTRÓFAVÉDELMI RENDSZER SZERVEZETI ÉS MŰKÖDÉSI SZABÁLYZATA MH Budapest, 2008

[3] HONVÉDELMI ÁGAZATI KATASZTRÓFAVÉDELMI TERV; MH Budapest, 2012

[4] 23/2005 (VI.16) HM rendelet a honvédelmi ágazat katasztrófák elleni védekezésének irányításáról és feladatairól (a 15/2011 (XI.15) HM rendelettel módosítva).

[5] EPR- Method -2003 „Method for Developing Arrangements for Response to a Nuclear or Radiological EmergencyAppendix: Plans and procedures; IAEA, Vienna 2003 p.190 ISBN 92–0–111503–2

[6] ORSZÁGOS BALESET- ELHÁRÍTÁSI INTÉZKEDÉSI TERV 5.1 SZÁMÚ ÚTMUTATÓ 1. VERZIÓ p.28. Országos Atomenergia Hivatal, Budapest 2008

[7] 2011. évi CXIII törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről.

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Tamási Béla – Grósz Zoltán
bela.tamasi@hm.gov.hu – grosz.zoltan@uni-nke.hu

NUCLEAR SECURITY – THE ROLE OF THE ENGINEER AT NUCLEAR POWER PLANTS

Absztrakt/Abstract

Minden ország alapvető kötelessége, hogy megóvja a kritikus infrastruktúrák körébe sorolt atomerőműveit, amely során feladatuk biztosítani a környezet megóvását az esetlegesen bekövetkező nukleáris balesetek esetében. A veszélyes nukleáris anyaggal üzemelő erőműveknek működésük során szigorú biztonsági követelményeknek kell megfelelniük. A képzett mérnökök az erőművek biztonságát és a környezet védelmét ötlépcsős műszaki alkalmazással valósítják meg. Az erőművek tervezése során a „mélységi védelem" megvalósítása alapvető követelmény. Ennek során a mérnökök kizárólag olyan erőműveket tervezhetnek, amelyek a katasztrófák negatív hatásainak ellenállnak és az üzemzavarokat is megfelelően tudják kezelni. Vajon, a magas szintű technológiák alkalmazásával elkerülhetőek a nukleáris balesetek?

Each country's fundamental duty is to protect nuclear power plants categorised as critical infrastructure and to ensure the preservation of the environment in case of nuclear accidents. Due to the unstable nature of the materials used within nuclear power plants safety measures utilized by the nuclear energy industry must be rigorous. Highly skilled engineers follow a five step approach to deliver the virtual defence in depth required to maintain a safe and secure environment within a nuclear power plant. One of the fundamental tenets of nuclear power plant design is "Defence in Depth." This approach leads engineers to design a plant that can withstand severe catastrophes, even when several systems fail. Will applying these hi-tech methods really help us avoid nuclear accidents?

Kulcsszavak/Keywords: *nukleárisbiztonság, biztonságosüzemeltetés, biztonságifunkciók, mélységivédelem, biztonságigátak, biztonságirendszerek ~ nuclear security, safety operation, security functions, virtual defence in depth, security measures, security systems*

1. INTRODUCTION

Nuclear power plants are spread all over the world and are involved in the energy production of approximately 30 countries. The world now has 435 operating nuclear power plant units in 190 nuclear power plants.[1]

Reactors however – regardless of their type – have unique design, there are no two nuclear power plants in the world that are the same in every detail. Safety systems of nuclear reactors, just like everything else in the world, are continuously developing. There is more experience in this field for which a high price has been paid unfortunately, since they were obtained at the expense of accidents. It is very important to understand that regardless of the level of development of a nuclear reactor or its security system there is no 100 percent safety or guarantee for safety. The most important thing a security system of a nuclear power plant has to fulfill is to prevent the release of radioactivity into the environment. Let's see how it could be implemented. [1]

2. SAFETY AND THE SAFETY OF NUCLEAR POWER PLANTS

In Hungary, long-term or permanent failure of electric energy production – technically speaking: production safety emergency – may cause a serious electricity supply problem, a temporary energy crisis. The economic damage due to "production safety emergency" means that although a nuclear emergency situation[2] does not exist, but one or more blocks of the nuclear power plant are out of production, or other major economic damage happened that does not affect the production.

The word safety is very often used in everyday life. The meaning of it in general terms and in technical terms is defined as follows[3].

Security is:

- The basic needs of existence and subjective experience and / or in existential situationswhen the person is not threatened by any kind of danger, or if it so, it can be avoided.
- (Technical) strength of a building, machinery, structure, or the safe and smooth operation of it, or the nature of them that they are harmless to the environment in the vicinity or it does not threaten the safety of the occupants. Security is always relative, which means that only among certain environmental conditions or under the maximum output exists. [2]

Studying these two conditions – namely "certain environmental conditions", and "under the maximum output" – from the perspective of nuclear safety, we can determine the safety concept of nuclear power plant, scilicet: safety is that quality of the plant's characteristics, which provides protection for the operational staff and for the public against external and internal exposure, prevention of radioactive contamination of the environment, the avoidance of exceeding the permissible exposure limits written in the relevant standards for either stationary or in emergency situations.

[1] Source: IAEA March 18 2011
[2] means: by radioactive or/and nuclear material caused contamination
[3] Magyar Nagylexikon, AkadémiaiKiadó, Budapest, 1995.

2.1 The safety of nuclear power plants

"Science and technology – I want to say that very clearly – does not solve every problem but without science and technology can not be solved any problem."[4]

The safety level of nuclear power plants nowadays is much higher than twenty years ago. The anachronism of the old developments from the perspective of security and the two major reactor accidents with significant implications – Three Miles Island in 1979 and Chernobyl in 1986 (see below) – has prompted the nuclear power plant owners to significantly increase the safety level of their plants. Therefore, the reactors operating these days are equipped with multiple safety systems. The safety of nuclear power stations means that the plants must be designed with every technical equipment and security system able to guarantee the safety of the plant's environment, in case of a major accident. The review of the security and the continuous development to improve it is an elementary requirement from the owners.

The Government of Hungary delegated control of the nuclear power station to the National Nuclear Energy Authority, similarly to the other nuclear facilities (KFKI Research Reactor, BME Training Reactor, Irradiated Cassettes Transition Storage Facility etc).

The implementation of nuclear safety starts with the planning of the nuclear power plant: it must be built and operated in such way that in case of an accident it guarantees the safety of the environment.Through the operation it should make every effort to increase its' security. It is based on regular overview and reassessment of the security situation in order to ensure that the new scientific achievement and operating experience of other plants are utilized in every nuclear power plant. [3]

2.2. For the safe operation

The safe operation of a nuclear power plants is one of the most important criteria. There is a large amount of radioactive material in a nuclear reactor and against it's radiation the facility staff must be protected. In case of an accident leakage must be prevented.

In the nuclear reactor three basic conditions must be fulfilled.These are:

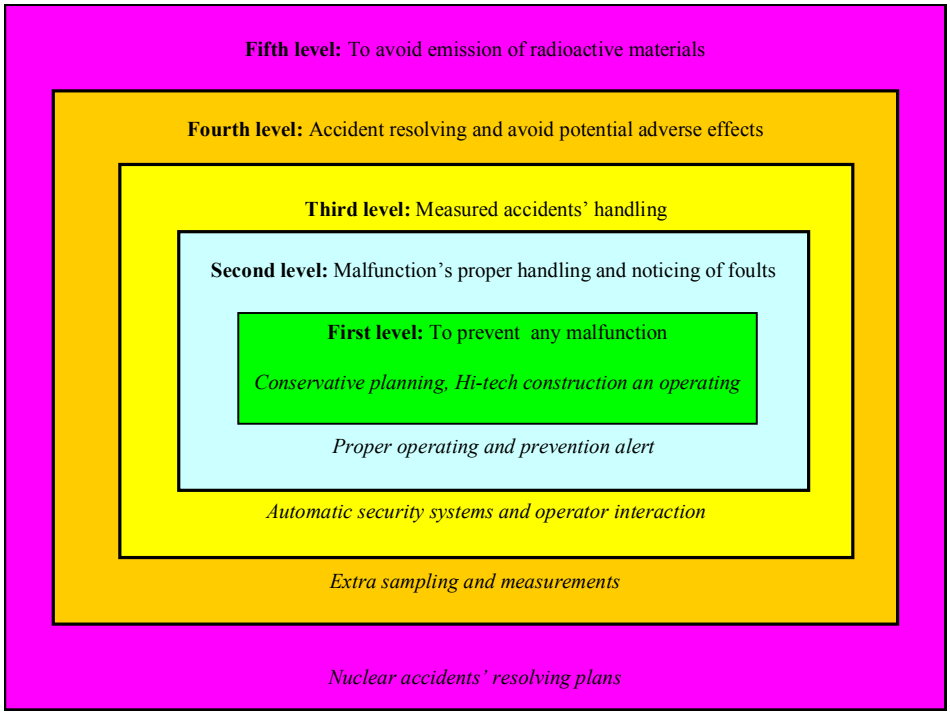
- effective control of the nuclear chain reaction;
- the proper conveyance of generated power;
- prevention of the loss of radioactive material.

The safety functions of nuclear reactors are implemented using the so called ”defence in depth”.

3. THE DEFENCE IN DEPTH

This is a theory developed in the 1990s by the International Nuclear Energy Agency. Every country's authority has to enforce greater effect of this principle. The defence in depth is linked to the relevant level of the above mentioned three conditions. The five levels of defence in depth principle settle the security-related offenses, equipment, procedures. Each is designed to prevent to achieve the next level. [4] (see Figure 1.)

[4] Teller Ede: A biztonságbizonytalansága



1. figure. "Virtual defence in depth"
Forrás: www.agr.unideb.hu/ktvbsc/dl2.php?dl=17/14_eloadas.ppt; (2011. október 24.)

First level: The entire plant must be designed so that it's resistance against the internal faults is the greatest possible or these errors occurs least frequent possible. Then on this basis, the facility must be designed, to ensure of course an adequate safety margin of error. The possibility of human error must be excluded as much as possible or human-managed devices must be transparent and easy to operate. The workers must be selected for the job properly – taking into account the psychological stress also. It must be specified which external events are important to withstand without damage to the system. Another important factor is the selection of the site for future power plants. Clear responsibilities should be determined from the design phase to the operation.

Second level: The facility must be kept within the designed operating limits and a separate device must be provided to prevent any violation of safety constraints. Instruments like this are: constant measurements, periodic testing, constant maintenance, periodic testing of security systems. Care should be taken to display accurate operation of instrumentation, without any delay every error should be fixed, even if this results drops of production. Every effort should be taken in practice to eliminate errors which could be abolished theoretically.

Third level: The aim of the first two levels of defence in depth is to make smaller the chance for errors. In spite of this the potential for malfunctions and accidents can not be excluded. Therefore the system should be prepared for some so-called "plausible accidents". These "plausible accidents" derive from reasons that despite the constant controls can not be excluded. Therefore, we need systems that help manage the expected emergency situation. These security systems shall be designed so that they initiate automatically and human intervention is permitted only after a certain time – when the situation has been cleared, defined and reviewed. In case of any plausible accidents these systems maintain the integrity of the active zone.The leakage of radioactive substances are therefore, constrained to the proper level even in the case of the worst plausible accident.

Fourth level: The system must be prepared for worse case scenarios as well, which lead to accidents formerly classed as non-plausible or more than one error occurs at a time. In this case the security systems do not provide adequate protection, the most dangerous situation for the reactor may occur: “zone melting”, which is is accompanied by highly radioactive emissions. So the goal here is to reduce the chance of these kinds of events among the given conditions and to insert additional systems, which reduce the extent of the zone melting, or at least delay, allow time for any other action (such as evacuation of the population).

Fifth level: Provision must be taken for the event of radioactive emission. These measures are necessary just in case the first four levels’ measures proved ineffective. This level of course is not longer the responsibility of the plant, but requires authorities’ action. These tasks should be incorporated into a contingency plan and all the decisions should be based on this or on the opinion of the subject matter expert team. It is imperative to run the system smoothly in emergency situations, therefore periodic re-training shall take place with the involvement of the applicable agencies (eg: National Nuclear Energy Agency, Disaster, Health).

4. THE ENGINEERING BARRIERS (TECHNICAL SOLUTIONS)

The so-called ”engineering barriers“ prevent the leakage of radioactive substances into the environment either in normal or in emergency situations. The primary role of the certain dams is to prevent the radioactive material from reaching the next dam. The primary aim of safety analysis is to determine whether, these dams work properly in normal mode, in normal operations or in case of an emergency situation.

The first engineering dam is the fuel lozenge itself, the major part of fission products created during the operation embedded into the nuclear fuel matrix which would prevent their evasion.

The second engineering dam is the case of thenuclear fuel rod, in which the uranium dioxide pastilles are filled. These – mostly of zirconium alloy cases – are filled with inert gas and are hermetically sealed. Thus, the jacket locks the gaseous fission products. In normal mode the first two engineer dams are responsible for the retention of radioactive materials.

The third engineering dam in the reactor tank itself, within the tank is the active zone and the primary circuit. The stainless steel reactor tank is calibrated for extreme temperature and pressure thus in case of possible damage to the fuel it gives additional protection against leakage of radioactive materials into the environment.

The fourth engineering dam is the safety building itself that includes the entire primary coolant circuit, the containment, which is calibrated for the over pressure created during a so called scaling accident and continuously kept ventilated controlled manner through filters.

5. INTERNAL AND EXTERNAL SECURITYSYSTEMS

We can speak of internal or inherent safety, if the reactor is designed in such way that the increase of the reactor power reduces the reactivity of the reactor, so the number of the fissions, ergo the output itself. These negative feedback loops based on physical processes therefore it cannot be deactivated, so in case of an accident or in an emergency situation it protects the reactor in the so-called ”run away”.

The aim of the external security systems is to control the reactor’s output, to inactivate if necessary, to remove the released heat and to prevent the leakage of radioactive material. This latter function is fulfilled by the previously mentioned engineering dams. The chain reaction is stopped and controlled in the short term by the control rods, for long term boric acid

dissolved in the primary coolant is used. They absorb free neutrons in the reactor, thereby reducing the number of fissions. [5]

It is the nature of nuclear power plants that the heat generation in the reactor is not finished immediately after the chain reaction was terminated as the generated heat[5] previously to be released. Immediately after termination this residual heat is 7% of the nominal operating output which is decreasing as time passes. Because of this remanentheat effective cooling of the reactor is required not only during normal operation, but even after the termination. The emergency cooling systems are an important part of the external security systems because these perform this task even in the case of damage of the primary cooling circuit. The nuclear power plants nowadays are designed in such a way that even if the largest diameter primary circuit breaks[6] the cooling of the reactor can be provided adequately.

The safety systems are built multiple based on the principle of redundancy so that the defence system remains viable despite the failure of any element. The principle of diversity means that the parts of the system are produced by several different manufacturers or based on different principles of operation so that the common-mode failures can be avoided.

An important component of safety is the operator's commitment to security and the organization's safety culture. It can be strengthened by high standard continuous education of the operators and maintenance personnel and by the strong safety-awareness approach. It is basic criteria for operators of nuclear installations and their leaders that security is considered top priority, and that they remain vigilant in their daily work. The technical systems and the staff together can provide the required safety standards.

6. SECURITY FEATURES OF IMPLEMENTATION

The proper design, engineering dam and defence in depth are illustrated in the two worst nuclear power accidents and the description of the incident in Paks.In 1979 in the United States, in the second block of the Three Mile Island nuclear power plant after the loss of coolant and operator error caused partial zone melting. The melt, however, remained within the reactor tank. The containment fulfilled its function and retained the majority of the radioactive material. Only some radioactive inert gas emissions occurred, but this was only a negligible additional radiation caused to the population. [6]

The other accident was not as lucky. In the fourth block of the Chernobyl Nuclear Power Plant in April 1986 there was a serious reactor “run away” accident. Construction errors made the incident even worse since the reactor did not have negative feedback necessary for inherent security; on the top of it the external security system was deactivated and this led to a reactor explosion. The lack of a heavy duty reactor tank, suitable protective reactor building led to the absence of other safety means which are required in Hungarian or in the western reactors. This resulted in a large environmental release and the population radiation exposure was very significant. [7]

Speaking about nuclear safety, we have to mention the incident that occurred in April 2003 in the second block of the Paks Nuclear Power Plant. In a temporary installed underwater outside cleaning tank of the reactor, thirty heather cases were damaged. The damage was caused by inappropriate cooling. The residual heat was high and the cases became overheated and brittle thus after inundating flooding they became crumbled. Part of the gaseous radioactive fission products from the damaged nuclear case escaped into the environment (the first two engineering dams were damaged), but there was no significant contamination.

[5] or remained heat

[6] so called: pipe breaking or coolent-lost malfunction

7. THE FUKUSHIMA ACCIDENT FROM AN ENGINEER'S POINT OF VIEW

The earthquake that hit Japan in March 2011 was several times more powerful than the worst earthquake the nuclear power plant was built for. When the earthquake hit the nuclear reactors all automatically shut down. Within seconds after the earthquake started, the control rods had been inserted into the core and the nuclear chain reaction stopped. At this point, the cooling system should carry away the residual heat. The earthquake destroyed the external power supply of the nuclear reactor. This is a challenging accident for a nuclear power plant, and is referred to as a "loss of offsite power." The reactor and its backup systems are designed to handle this type of accident by including backup power systems to keep the coolant pumps working. Furthermore, since the power plant had been shut down, it cannot produce any electricity by itself.

For the first hour, the first set of multiple emergency diesel power generators started and provided the electricity that was needed. However, when the tsunami arrived it flooded the diesel generators, causing them to fail. A large tsunami that disables all the diesel generators at once is such a scenario, but the tsunami was beyond all expectations. When the diesel generators failed after the tsunami, the reactor operators switched to emergency battery power. After 8 hours, the batteries ran out, and the residual heat could not be carried away any more. At this point the plant operators begin to follow emergency procedures that are in place for a "loss of cooling event." These are procedural steps following the "Depth in Defence" approach. All of this, however shocking it seems to us, is part of the day-to-day training you go through as an operator.

At this time people started talking about the possibility of core meltdown,[7] because if cooling cannot be restored, the core will eventually melt (after several days), and will likely be contained in the containment. However, melting was a long way from happening and at this time, the primary goal was to manage the core while it was heating up, while ensuring that the fuel cladding remain intact and operational for as long as possible.

Because cooling the core is a priority, the reactor has a number of independent and diverse cooling systems such as the reactor water cleanup system, the decay heat removal, the reactor core isolating cooling, the standby liquid cooling system, and others that make up the emergency core cooling system.

Since the operators lost most of their cooling capabilities due to the loss of power, they had to use whatever cooling system capacity they had to get rid of as much heat as possible. But as long as the heat production exceeds the heat removal capacity, the pressure starts increasing as more water boils into steam. The priority now is to maintain the integrity of the fuel rods by keeping the temperature below 1200°C, as well as keeping the pressure at a manageable level. In order to maintain the pressure of the system at a manageable level, steam and other gases have to be released from time to time. This process is important during an accident so the pressure does not exceed what the components can handle, so the reactor pressure vessel and the containment structure are designed with several pressure relief valves. So to protect the integrity of the vessel and containment, the operators started venting steam from time to time to control the pressure.

During this time, mobile generators were transported to the site and some power was restored. However, more water was boiling off and being vented than was being added to the reactor, thus decreasing the cooling ability of the remaining cooling systems. At some stage during this venting process, the water level may have dropped below the top of the fuel rods. Regardless, the temperature of some of the fuel rod cladding exceeded 1200 °C, initiating a

[7] Note that the term "meltdown" has a vague definition. "Fuel failure" is a better term to describe the failure of the fuel rod barrier (Zircaloy).

reaction between the Zircaloy and water. This oxidizing reaction produces hydrogen gas, which mixes with the gas-steam mixture being vented. This is a known and anticipated process, but the amount of hydrogen gas produced was unknown because the operators didn't know the exact temperature of the fuel rods or the water level. Since hydrogen gas is extremely combustible, when enough hydrogen gas is mixed with air, it reacts with oxygen. If there is enough hydrogen gas, it will react rapidly, producing an explosion. At some point during the venting process enough hydrogen gas built up inside the containment (there is no air in the containment), so when it was vented to the air an explosion occurred. The explosion took place outside of the containment, but inside and around the reactor building there was no safety function.[8]

Since some of the fuel rod cladding exceeded 1200 °C, some fuel damage occurred. The nuclear material itself was still intact, but the surrounding Zircaloy shell had started failing. At this time, some of the radioactive fission products[9] started to mix with the water and steam that was released into the atmosphere.

Since the reactor's cooling capability was limited, and the water inventory in the reactor was decreasing, engineers decided to inject sea water[10] to ensure the rods remain covered with water. Although the reactor had been shut down, boric acid is added as a conservative measure to ensure the reactor stays shut down. Boric acid is also capable of trapping some of the remaining iodine in the water so that it cannot escape, however this trapping is not the primary function of the boric acid.

This process decreased the temperature of the fuel rods to a non-damaging level. Because the reactor had been shut down a long time ago, the decay heat had decreased to a significantly lower level, so the pressure in the plant stabilized, and venting was no longer required. [8]

8. CONCLUSION

To create a safe environment is the task of the operators of the power plant. It is well known that the radioactive material used in power plants has a risk itself to the environment. Having this knowledge the experts are working constantly to ensure nuclear safety. In our analysis we worked out of those technical solutions of the nuclear power plant whose task is during the operational function to prevent the escape of radioactive materials into the environment, thereby ensuring nuclear safety. We reviewed the interpretation of security, the implementation of the safety functions and finally we described the technical solutions used for preventing the leakage of radioactive substances into the environment. The safe operation of the large number of currently operating nuclear reactors in the world demonstrates the precise engineering calculations. "The nuclear energy in the hands of intelligent people is not dangerous."[11] As a matter of fact only one single nuclear accident – the one that happened last year at Fukushima – is able to radically change this view.

Felhasznált irodalom

[1] Aszódi Attila: ATOMERŐMŰVEK AVILLAMOSENERGIA-TERMELÉSBEN Magyar Tudomány 2007/01 p11. ISSN 0025-0325

[2] Holló Előd: ATOMERŐMŰVEK KOCKÁZATÁNAK ÉRTÉKELÉSE; Magyar Tudomány 2007/01 p19.*ISSN* 0025-0325

8This explosion destroyed the top and some of the sides of the reactor building, but did not damage the containment structure or the pressure vessel. While this was not an anticipated event, it happened outside the containment and did not pose a risk to the plant's safety structures.

9 e.g.cesium and iodine

10mixed with boric acid – a neutron absorber

11 source: Teller Ede: visit in Paks NPP

[3] BukovicsIstván - VavrikAntal: INFRASTRUKTÚRÁK KOCKÁZATA ÉS BIZTONSÁGA Hadmérnök I. Évfolyam 3. szám - 2006. december p9. ISSN 1788-1919

[4] Dr. Trampus Péter: A VIRTUÁLI MÉLYSÉGI VÉDELEM KONCEPCIÓ ALKALMAZÁSA A REAKTORTARTÁLY BIZTONSÁGÁNAK IGAZOLÁSÁRA Magyar Energetika 2005/1 ISSN 1216-8599

[5] Hamvas János: FIZIKUSOK A PAKSI ATOMERŐMŰBEN; Fizikai Szemle 2000/11. p 398. *ISSN* 0015-3257

[6] OPEN SOCIETY ARCHIVES; http://www.osaarchivum.org/guide/rip/10/TheExhibitionIII.html; (2011.október 14.)

[7] Kováts Balázs: A NUKLEÁRIS IPAR ÉS A TÁRSADALOM; Magyar Tudomány 2001/11 in1364-1367 *ISSN* 0025-0325 http://www.matud.iif.hu/01nov/kovats.html; (2011. október 21)

[8] Josef Oehmen: INFORMATION ABOUT THE INCIDENT AT THE FUKUSHIMA NUCLEAR PLANTS IN JAPAN; http://mitnse.com/2011/03/13/modified-version-of-original-post/; (2012. november 1.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Zsákai Róbert

A CUNAMI KIALAKULÁSÁNAK OKAI

Absztrakt

A cikk elsődleges célja, hogy a cunami okozta katasztrófa bemutatásával, ráirányítsa a figyelmet a katasztrófák megelőzésével, felszámolásával, a védekezés irányításával kapcsolatos feladatok fontosságára. Az utóbbi évtizedben, az emberek nagy része már nemcsak a távoli országokból érkező tudósításokból értesülhet természeti és ipari katasztrófák, elemi csapások okozta károkról, tragédiákról. Saját maga is megtapasztalhatja utazásai során, lakhelyén is, ezeknek az eseményeknek a sokkoló hatását. Vizsgálatom középpontjába a cunami kialakulásának okait, lehetséges következményeit helyeztem.
Katasztrófa bárhol is következik be, az mindig mindenhol tragédia. Mióta emberiség létezik, mindig védekezünk ellene, hol kevesebb, hol nagyobb sikerrel.

By presenting the disaster caused by the tsunami, the primary target of this article is to draw the attention to the importance of tasks in connection with the prevention, liquidation and the management of the protection. In the past decade most of people hear about damages, catastrophes caused by natural and industrial disasters, acts of God from reports coming not anymore only from far countries. People can experience them the shocking effect of these events during their travelling, and at their living place as well. In my analysis I have focused on the reasons of the formation of a tsunami and its potential consequences. It is always a tragedy if a disaster happens at any place. Since the mankind has been existing, we have always been on defensive against it, sometimes with more, sometimes with less results.

Kulcsszavak: *katasztrófa, földrengéses övezetek, tengeri hullámfajták, cunami ~ catastrophe, earth quake zones, sea wave types, tsunami*

1. BEVEZETÉS

Napjainkban egyre több veszélyforrásnak vagyunk kitéve, amelyek megjelenhetnek mindennapjainkban is. Ezekre ma már tudatosan kell, vagy kellene felkészülnie minden nemzetnek és társadalomnak. Alapvető kérdés, hogy rendelkezünk–e azokkal az ismeretekkel, melyek segítségével megmenthetjük magunk és mások életét? A főként megelőzésre irányuló, új szemléletű információs kampányokat minél szélesebb körben próbálják a szakemberek eljuttatni az állampolgárok felé, legyen szó egészségügyről, katasztrófáról, tűzmegelőzésről, bűnmegelőzésről, stb. De vajon célt érnek-e az információk és kellő hatásúak? Rohamosan fejlődő világunkban ezek a folytonosan megújuló információkat hogyan fordíthatnánk a lakosság javára?

2. A KATASZTRÓFÁK FAJTÁI

A katasztrófák feloszthatók időtartamuk, kialakulásuk sebessége, térbeli kiterjedésük, az általuk érintett személyek száma, az okozott kár nagysága, az azokat kiváltó okok eredete és ismertetőjegyei, és még sok egyéb megfontolás alapján. A meghatározó szempont az egyes katasztrófák eredete, illetve kiváltó oka. A *katasztrófa* görög eredetű szó, fordulat, megsemmisülés, csapás, megrázó hirtelen esemény, az emberi élet, az anyagi javak, természeti értékek pusztulása. Fogalmának meghatározása során különböző megközelítésekkel találkozunk. [1] Hasonló értelmű az ugyancsak görög eredetű krízis szavunk is, mely fordulópontot, súlyos átmeneti állapotot jelent. A külföldi szakirodalmak általában szinonimaként említik e két kifejezést. A magyar köznyelv különbséget tesz a két fogalom között. A katasztrófa a már bekövetkezett, visszavonhatatlan tragédia, míg a krízis egy fordulópont előtti állapotot jelöl.

A katasztrófák két fő csoportba sorolhatók: civilizációs és természeti katasztrófák.

2.1. Civilizációs katasztrófák

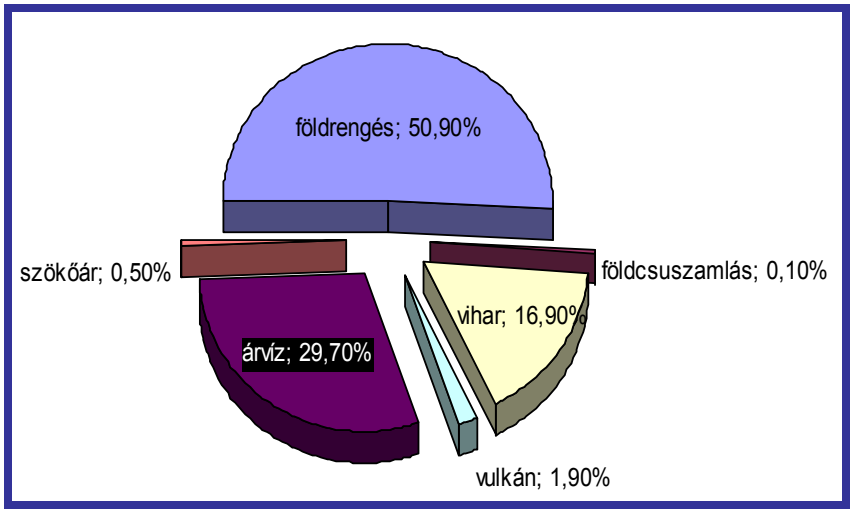
„Ebbe a kategóriába, azok a katasztrófák sorolhatók, amelyek kialakulásának előfeltétele a civilizáció léte, a tudomány, a technika, az ipari és mezőgazdasági termelés, a közlekedés, és a szállítás meghatározott szintje.” [2, p. 17]

A civilizációs katasztrófák alapvető jellemzője, hogy emberi tevékenységgel függenek össze, amelyek helytelen emberi beavatkozás, mulasztás, szándékosság, vagy technikai hibák hatására következnek be, pl.: üzemzavar, közúti baleset, veszélyes anyag kiszabadulása. Ebbe a kategóriába tartozik a társadalmi katasztrófák legnagyobbika, a háború is. A civilizációs veszélyhelyzetekre való felkészülés, egyre nehezebb és sokrétűbb tervezést, szervezést igényel, kiszámíthatatlansága miatt is. Egy lehetséges válasz az ilyen típusú kihívásokra a katasztrófavédelem rendszere.

2.2. Természeti katasztrófák

A természeti katasztrófák közös jellemzője, hogy általában emberi beavatkozás nélkül, a természet erőinek hatására alakulnak ki. A természeti katasztrófákkal szemben az ember kiszolgáltatott, kialakulását, bekövetkezését nem, vagy csak ritkán tudja megakadályozni, tehát az emberi tevékenységtől függetlenül, a természet erőinek hatására elemi csapásként fordulnak elő. *(1. ábra)*. A természeti katasztrófák között vannak határesetek, amelyek a természeti erők hatására és emberi beavatkozás következményeként jönnek létre. [3]

Ilyen például az árvíz és belvíz, melyet geológiai, vagy meteorológiai okok egyaránt előidézhetnek. Mindezeken túl, vagy ezekkel párhuzamosan, az emberi mulasztás is előidézheti ezt a katasztrófát. Árvízről akkor beszélünk, ha a folyó kilép a medréből, és elönti a környező településeket.



1. ábra. Természetes katasztrófák áldozatai a XX. században (összesen kb. 4 millió)
Forrás: http://www.matud.iif.hu/07maj/07.html; (2011. 01. 12.)

Az elmúlt évszázadban több mint négymillió ember vesztette életét a Földön természetes katasztrófák során, közülük valamivel több, mint a fele földrengések következtében halt meg. Az ábrán jól látható még, hogy az árvizek is hatalmas pusztításokat okoztak, ezért hazánknak is fontos feladata a katasztrófa-elhárítás. Magyarországot is érintő belvizek kialakulása részben előre jelezhető. Az ilyen típusú katasztrófánál is fontos a megfelelő veszélyhelyzet-kezelés, és a helyes magatartási formák alkalmazása.

Nem lehet előre jelezni a földrengést, villámcsapást, aszályt, melynél megfigyelhető, hogy nagyobb kárt okoz a felkészületlenség, mint maga a katasztrófa.

Mivel a természeti erők közül a földrengés az egyik legpusztítóbb katasztrófa-és közvetve ez is okozhatja a cunami jelenséget.

3. FÖLDRENGÉSES ÖVEZETEK

A tudósok már azelőtt elkezdték feltérképezni, hol gyakoriak a földrengések, hogy megértették volna, mi okozza őket. [4]

Földrengések a világon mindenütt előfordulhatnak, mégis általában a lemezhatárokhoz közeli területeken a leggyakoribbak. Ezek közül az egyik leghíresebb a Szent András-törés; ez az Egyesült Államok nyugati partvidékén húzódik, és belőle indulnak ki a kaliforniai földrengések. Sok törésvonal halad Kína és Japán környékén is. Kobe például a Nojima-törésre esik.

A legtöbb földrengés csak néhány másodpercig tart, de van olyan is, amelyik egy percig vagy még tovább. A San Franciscó-i földrengés 40 másodperces, az Alaszkát megrázó 1964. január 24-i viszont több mint 7 perces volt.

1755-ben egy földrengés után a portugáliai Lisszabonra 17 méter magas hullám zúdult, s a földrengés utórezgései földcsuszamlást és tüzet okoztak. Elpusztult az épületek háromnegyede, és 60 ezer ember vesztette életét. Ahogy egyre pontosabbá váltak a mérési módszerek a földrengések helyének meghatározására, egyre jobbak lettek a földrengéstérképek is, és sokkal részletesebb kép rajzolódhatott ki a szeizmikus tevékenységről. [5]

A Föld szakadatlanul mozog, de szerencsére ritkák a katasztrofális földrengések. A földrengések szakértői, a szeizmológusok évente mintegy ötszázezer földrengést regisztrálnak, azaz szinte percenként egyet-egyet. Ezeknek a rezgéseknek a többsége észrevétlen marad, csak a szeizmológusok szereznek róluk tudomást, igen érzékeny

műszerük, a szeizmográf révén. A legtöbb földrengés nem vált ki cunamit, ezért van szükség az észlelőbójákra, amelyek a tengerszint magasságának változásait jelzik. A bóják az információt a műholdaknak, azok pedig a vett jeleket a feldolgozó központba továbbítják.

Földrengés akkor támad, ha a törésvonalon levő kőzetek a lemezek összeütközésével felgyűlt nyomás alatt meghajlanak. Régebben a kiszabadult energia mennyiségét, egy amerikai kutatóról elnevezett skálával, a Richter-skálával mérték.

A fő rengést néha több, egyre kisebb erősségű utórengés követi. Az utórengéseket az okozza, hogy a széttöredezett kőzetek felveszik új, stabil helyzetüket, s még ezek a rengések is nagyon nagy pusztítást idézhetnek elő. 1985-ben Mexikóvárosban, a városközpontban hatalmas rombolást végzett egy, a Mercalli-skála szerint 11-es erősségű földrengés. A másnapi utórengés 10-es erősségű volt, azt is tönkretette, ami az előző nap megmaradt. A két földrengés együtt 10 ezer ember halálát okozta, és romba döntötte a nagyváros tömérdek épületét.

Sok földrengés úgy mozgatja a talajt, mintha az imbolygó hajófedélzet volna. A talaj a földrengés erősségétől függően lágyan hullámzik, vagy hevesen ide-oda rándul. Időnként a földrengéshullámok a felszínen is meglátszanak. A földrengések keletkezési mechanizmusairól már sokat tudunk, de nem tudjuk azonban előre jelezni a földrengések kipattanási idejét. Ez ugyanis sok tényezőtől függ, és a folyamat annyira bonyolult, hogy a legtöbb kutató véleménye szerint pontos előrejelzésre sohasem lesz mód. A földrengésveszély ismeretében azonban előzetes felkészüléssel, jelentősen csökkenthetők a rengések által okozott károk. [6]

A legveszélyesebb földrengések a tengeri rengések, melyek hatalmas cunamikat idézhetnek elő. Rendkívül nagy hullámhosszú és periódusidejű hullám. Amikor a cunami a part felé halad, akkor a tenger előbb visszahúzódik, majd hatalmas hullámok sorozatával árasztja el a partot. A cunami amplitudója a nyílt tengeren csak deciméter nagyságú, a periódusideje és a hullámhossza meghaladhatja az 500 km-t. A hullámok keskeny öblökbe beszorulva 20 méter magasra is felemelkedhetnek, s elsöpörnek mindent, ami az útjukba kerül.

4. TENGERI HULLÁMFAJTÁK

A cunami japán szó, a "cu" jelentése part, a "nami" hullámot jelent, tehát „parti hullám”. Az óceánokon és tengereken háromféle hullámot lehet megkülönböztetni. Leggyakoribb a szél által keltett "normális" hullám, de az árapály jelensége is hullámot kelt. Végül maga a cunami is hullám, illetve hullámok sorozata. E három hullámfajta tulajdonságai alapvetően eltérnek egymástól.

- A szél által keltett hullámok maximum 8-10 méter mélységig nyúlnak le, amplitúdójuk nem haladja meg a 20 métert, 100-500 méteres hullámhossz mellett 20-50 km/óra sebességgel terjednek.
- Az árapályhullám 10-30 méter mélyre terjed, amplitúdója 2-10 méter, hullámhossza 1-2 km, terjedési sebessége 20-40 km/óra.
- A fentiektől alapvetően eltér a cunami, hiszen az egész víztömeg megmozdul, amplitúdója csupán 0,4- 2 méter, hullámhossza viszont 100-300 km és terjedési sebessége 500-1000 km/óra. Különösen összeszőkülő öblökben érhet el nagy magasságot. A hatalmas víztömeg egyirányú mozgása miatt a hatása közismerten katasztrofális lehet.

4.1. Cunamik kialakulásának okai

Jelenlegi ismereteink szerint cunamikat négyféle jelenség hozhat létre:

- Tenger alatti földrengések.
- Vulkáni szigeteken bekövetkező robbanásszerű vulkáni kitörések, amelyek következtében a vulkáni építmény összeomlik, és helyét tenger önti el.
- Nagyméretű tengeralatti földcsuszamlások.
- Különösen nagy meteorit vagy aszteroida becsapódása a tengerbe.

4.1.1. A „tengerrengés”

Bár tapasztalatok szerint a legtöbb cunamit tenger alatti földrengések hozzák létre, az is kiderült, hogy nem minden tenger alatti földrengés okoz pusztító szökőárt. Úgy tűnik, ha a földrengés hatására a tengerfenék csak oldalirányban mozdul el, nem jön létre cunami. Ha viszont a földrengés alkalmával a tengerfenék több métert megemelkedik, vagy lesüllyed, úgy kialakulhat a tengerrengés és ennek következtében a tengerparton a pusztító hullám *(2. ábra)*. Tenger alatti vulkáni kitörések is létrehozhatnak cunamikat. A tenger alatti földcsuszamlások szerepének mértéke még nem tisztázott. Valószínű, hogy ezeket is tenger alatti földrengések váltják ki.

2. ábra. A földrengés keltette cunami által leginkább érintett országok
http://www.mindentudas.hu/mindentudasegyeteme/20050109cunami.html; (2010. 09. 22.)

4.1.2. Vulkán a tengerben

A tűzhányók a földkéreg gyenge pontjain keletkeznek. A Földet egy kemény külső réteg, a litoszféra fogja körül, s ez a kéregből és köpeny szilárd részéből áll. A litoszféra hatalmas merev tömbökre, úgynevezett kéreglemezekre oszlik. Ezek a lemezek mély árkokban az alattuk lévő óriási nyomás következtében állandó mozgásban vannak. Egyes helyeken a mozgás hegyláncokat hoz létre, máshol a táblák mély árkokban esnek vissza a föld belsejébe. Ezek a táblák néha találkoznak, néha elszakadnak egymástól és a Föld kérgén egy-egy gyenge pontnak számítanak, ahol várhatóak a tűzhányókitörések.

A szakértők szerint több vulkántípust is megkülönböztethetünk, melyek kitörése nem egyforma. A cunamit előidéző vulkánkitörésre a Krakatau 1887-es kitörésekor volt példa. A Krakatau egy víz alatti vulkán, Jáva és Szumátra között. 1883 előtt csak pár sziklasziget állt ki a tetejéből. A víz alatt azonban egy 8000 méter magas tűzhányó rejtőzött, csúcsán hatalmas kalderával. A lesüllyedt kaldera körül másodlagos kráterek nyíltak. [7] Maga a vulkán kitörése is pusztító volt – a légnyomás házakat döntött le és a vulkáni hamu és por a kitörés központjától több szár méteres körzetben szétterjedt –de a legnagyobb kárt mégis a hatalmas,

15 méteres hullámok okozták, melyek rettentő erősséggel zúdultak a szomszédos Jáva és Szumátra szigetekre. A természeti katasztrófában 36000 ember vesztette életét. [8] Az erős csapás következtében Telok-Betong város teljesen eltűnt.

4.1.3. Tengeralatti földcsuszamlások

Máig vita tárgyát képezi, mi okozza a tenger alatti földcsuszamlásokat, de azért érdeklik a kutatókat, mivel azok néha nagyobb szökőárakat generálnak. A fent felsorolt jelenségek elsősorban az egymáshoz közeledő lemezszegélyek találkozásánál pattannak ki, s a Csendes- és Indiai-óceán partvidéke zömmel ilyen terület. Ezzel szemben az Atlanti-óceán medencéjére a távolodó lemezszegélyek jellemzők, amelyek esetében jóval ritkábban történnek hasonló események. *Mégis, egy kutatócsoport szerint 2300 évvel ezelőtt jelentős cunami pusztított végig a mai New York területén***.** Az óriáshullám kagylókkal és vastag üledékrétekkel borította Long Island és New Jersey területét, valamint fatörmelékkel borította be a Hudson-folyó partvidékét. Egy 60 ezer évvel ezelőtti, tenger alatti földcsuszamlást fedeztek fel bristoli kutatók az afrikai part mentén is. A homok- és sárfolyam mintegy 1500 kilométert tett meg egy némileg lankás tengerfenéken, kezdeti sebessége a másodpercenkénti 20 métert is elérhette. [9]

4.1.4 Meteorit vagy aszteroida becsapódása a tengerbe

Az *1950DA* jelű kisbolygót 1950. február 23-án fedezték fel. Azóta, fél évszázadon át figyelték optikai távcsövekkel, most pedig radarméréseket végeztek rajta, az eddiginél sokkal pontosabban határozva meg a pozícióját. A nagyon pontos mérések szerint 0,33% (vagyis 1/300) vagy annál kisebb a kockázata, hogy 878 év múlva a kisbolygó eltalálja a Földet. Ez nagyobb kockázat, mint az összes többi ismert földközeli kisbolygó ütközési valószínűsége együttvéve.

Mi lenne, ha az ütközés tényleg bekövetkezne? Nagy szerencsétlenség lenne, de nem világkatasztrófa. A kutatók számítógéppel modellezték az aszteroida esetleges becsapódását. A szimulációban az aszteroida az Atlanti-óceánba zuhant, körülbelül 600 kilométerre az amerikai partoktól (a valóságban is nagyjából itt történne a becsapódás). Az ütközés hatása egy 60 ezer megatonnás TNT bomba robbanóerejével lenne egyenlő, és egy csaknem 20 kilométer átmérőjű körben teljesen kiszorítaná a vizet, egészen az 5 kilométer mély tengerfenékig, sőt még az aljába is krátert vájna. Ezután minden irányba elindulnának a hullámok, az elsők még kisebbek, de azután egyre magasabbak érkeznének, 3-4 percenként. A hullámok végigsöpörnének az Atlanti-óceánon és a Karib-térségen. Két órával a becsapódást követően 120 méteres hullámok érnék el Amerika keleti partjait, két órával ezután már a teljes partvonalon legalább 60 méteres hullámok söpörnének végig. Európába 8 óra alatt érne el a szökőár, 10-15 méteres hullámok formájában. A hullámok földcsuszamlásokat okozhatnak a tengerfenéken is, ami másodlagos szökőárakhoz is vezethet. [9]

5. KÖVETKEZTETÉSEK

A 2004. december 26-án bekövetkezett cunami óta rengeteg újságcikk, rádió- és tévéműsor látott napvilágot, sokszor ellentmondásos értékelésekkel. Ennyi év elteltével, talán elegendő információ áll rendelkezésünkre, hogy e borzalmas természeti katasztrófát, objektíven tudjuk megvizsgálni. Szakértők szerint is fontos az előrejelző-rendszer kiépítése, de az érintett lakosság felkészítése még fontosabb. Pozitívumként azonban már most megemlíthetjük, a katasztrófa menedzsment megjelenését, fejlődését, melyet már hazánkban is nyomon lehet követni. Hazánkban is, a Magyar Honvédség feladatai között is várhatóan a jövőben még komolyabb teret kap a katasztrófák kezelése, hiszen a katasztrófák kiszámíthatatlansági tényezőivel folyamatosan számolnunk kell.

Felhasznált irodalom

[1] http://www.edis.hu/?pageid=tudastar_alapfogalmak;

[2] Polgári védelmi ismeretek, önkormányzatok és polgári és védelmi szervezetek felkészítési segédlete. –Szolnok: Jász- Nagykun- Szolnok Megyei Polgári Védelmi Szövetség. 2002. – p. 17.

[3] Nagy László**:** Természeti katasztrófák. – Budapest, Lilliput, 1992.

[4] Jane Walker: Földrengések (történetük, kialakulásuk, és hatásuk az emberre). Bp.: Kossuth K., 1992. pp. 14- 25. –ISBN: 963-7839-11-9.

[5] Tudás Fája**:** Földrengések, 2000. pp. 28- 30. ISBN nélkül

[6] Tóth László: Japán, a földrengés és szökőár országa. História. 2011/4.pp.21.

[7] Horti József: Katasztrófák a természetben,1984.pp.52-53.

[8] Daniel Glick: Földünk vészjelei, In: National Geographic, szeptember, 2004. Sanoma Budapest Kiadói Kft. Budapest, pp. 39- 50. ISSN: 1589-3669

[9] http://www.mezogazd-sellye.sulinet.hu/docs/mindentudas/cunami/cunami.htm; (2011. 03. 12)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Duka Péter
alltea3@gmail.com

AZ ITSO SZABVÁNYBAN ALKALMAZOTT NXP MIFARE KÁRTYÁK ELLEN ALKALMAZOTT TÁMADÁSI MÓDSZEREK

Absztrakt

Napjaink gyors fejlődésének köszönhetően a proximity kártyás olvasók egyre jobban beépülnek a mindennapokba, a világon mindenhol. Egyre modernebb, és biztonságosabb technológiákat fejlesztenek ki a tudósok és szakemberek. Azonban a fejlődéssel a „cyber világ" bűnözői lépést tartanak, erre jó példa a cikkben bemutatott nagybiztonságú Mifare kártyák elleni alkalmazott sikeres támadási módszerek.

Thanks to the quick development of the modern age, the proximity readers increasingly spread on the whole world. The scientists and specialists develops better and safer technologies. The criminalist of the cyber world keep up with the development, a good example for this is the attacks against the highly secure Mifare memory cards showed in this article.

Kulcsszavak: *proximity kártyás olvasó, Mifare kártya ~ proximity reader, Mifare memory card*

1. BEVEZETÉS

Az ITSO *(International Transport Smartcard Organization)* egy nonprofit célú szervezet, mely az ITSO specifikációk kidolgozásáért felelős, alapítása pedig egészen 1998-ig vezethető vissza. Az ITSO tehát egy nyílt szabványcsomagot nyújt, mely lehetővé teszi a felhasználók számára a tömegközlekedésben használatos elektronikus eszközök és rendszerek interoperábilis használatát. Az interoperabilitás azt jelenti, hogy egy adott országon belül, vagy akár más országokban egyetlen elektronikus kártya segítségével több szolgáltatás érhető el számunkra. Pl. egyetlen RFID *(Radio Frequency IDentification)* kártyánk elláthat bérlet funkciót és elektronikus pénztárca funkciót.

Az ITSO nyílt szabvány a következő szabványokra épül:

- ISO/IEC 7816: Kontaktussal rendelkező smart kártyákra vonatkozó szabvány.
- ISO/IEC 14443: Kontaktus nélküli (proxy) kártyákra vonatkozó szabvány.
- ISO/DIS 24014-1:Az interoperábilis közlekedési rendszer struktúrájára, és a rendszer menedzselésére vonatkozó szabvány.
- EN 1545: Adatelemekre, felépítésre vonatkozó szabvány.

Az ITSO alapjában véve az ISO/IEC 144431 A típusú szabványra épülő kártyák használatosak, – Pl. Mifare Classic 1K, DESFire, stb. -, de támogatja a B típusú, nagyobb biztonsággal rendelkező kártyákat is.

Továbbá az ITSO biztonsági modulja (SAM = Secure Application Module) megfelel a nemzetközileg elismert szabálygyűjtemény, a Common Criteria EAL 4-es megfelelési szintjének. Az EAL 4 szint jelentése: tervszerűen tervezve, tesztelve és megvizsgálva. (7 megfelelési szint létezik, minél nagyobb a szám annál költségesebb egy rendszer.)

A kártyák titkosítására a DES2 és 3DES-t alkalmazzák, ritkábban az AES3-t.

2. A KÁRTYÁKON ALKALMAZOTT TITKOSÍTÁSI FORMA BEMUTATÁSA

A legtöbb kártyán a szimmetrikus kulcsú DES[4] és 3DES titkosítást használják, ritkábban az AES[5]-t. Több célszámítógépet is kidolgoztak e kódok feltörésére. A feltöréshez szükséges idő egy DES titkosítás esetében mindössze néhány óra, ugyanakkor egy AES kód esetében a feltörés napjainkban még megoldhatatlan feladat.

A továbbiakban – az ITSO rendszereken belül túlnyomó részben alkalmazott *(a világon több mint 70%-ban használt)* – NXP *(Philips leányvállalata)* Mifare kártyákról lesz részletesebben szó, azon belül is a leggyakrabban használt Classic típusról. *(Fontos*

---

1 ISO/IEC 14443 specifikációk:
14443-2: modulációs eljárásra, és kódolásra vonatkozó sémák.
14443-3: ütközés elkerülésre (anti collison) vonatkozó sémák.
14443-4: kommunikációs protokoll leírása.

2 DES, 3DES: Data Encryption Standard
Szimmetrikus kulcsú kódolás. Manapság a DES megerősítését, a 3DES-t alkalmazzák, mely a DES kódolás végrehajtása 3-szor egymásután. Tehát az (X=1…3)DES sorra 64, 128 és 192 bites kulcsokat alkalmaz.

3 AES: Advanced Encryption Standard
Hivatalosan az USA Szabványügyi és Technológiai Intézete (National Institute of Standardisation and Technology) fogadta el 2001-ben, és váltotta le az elavultnak számító DES-t. Azonban továbbra is gyakorta alkalmazzák az olcsóbb rendszerekben az egyszerűbbnek számító DES-t.

4 Data Encryption Standard
Szimmetrikus kulcsú kódolás. Manapság a DES megerősítését, a 3DES-t alkalmazzák, mely a DES kódolás végrehajtása 3-szor egymásután. Tehát az (X=1…3)DES sorra 64, 128 és 192 bites kulcsokat alkalmaz.

5 Advanced Encryption Standard
Hivatalosan az USA Szabványügyi és Technológiai Intézete (National Institute of Standardisation and Technology) fogadta el 2001-ben, és váltotta le az elavultnak számító DES-t. Azonban továbbra is gyakorta alkalmazzák az olcsóbb rendszerekben az egyszerűbbnek számító DES-t.

megjegyezni, hogy a Mifare Classic kártya nem smart card, tehát nem rendelkezik önálló mikroprocesszorral, hanem csak egy memóriakártya.) A feltöréseket legnagyobb számban e kártyák ellen hajtották végbe, mivel a szabványokban nem határozzák meg a szükséges védelmi szinteket, vagy akár a kölcsönös hitelesítést ezen olcsó kártyákra vonatkozóan. *(Pl. a Calypso tömegközlekedési nyílt szabványban alkalmazott kártyák ugyan drágábbak, de hibatűrőbbek, megtalálható a kölcsönös hitelesítés az alkalmazott kártya intelligenciája miatt, továbbá feltörés védettebb a rendszer is.)*

3. KOMMUNIKÁCIÓ

Először ismerjük meg az alkalmazott szabvány *(ISO/IEC 14443 [6]A típus)* a kártyára és az olvasóra vonatkozó főbb jellemzőket.

Olvasótól a kártya felé irányuló kommunikáció jellemzői a következők:

100%-os ASK modulációt használ, módosított Miller [7]kóddal. A kommunikáció sebessége 106 kbit/sec. A modulációs impulzusok szélesség 2,28µs, ez lehetővé teszi a passzív[8] kártya energiával való ellátását.

A kártyától az olvasó felé irányuló kommunikáció jellemzői:

Manchester-kódolást[9] alkalmaznak a bitek megkülönböztetéséhez. 847,5Khz-es vivőfrekvenciával. *(Egész számú többszöröse a kommunikációra használt 13,567Mhz-es frekvenciának.)* Az adatokat a kártya az olvasó erőterébe kerülve ellenállásuk megváltoztatásával *(Az olvasó és a kártya tekercsantennája között induktív kapcsolat áll fent. Ennek folytán a kártyába beépített terhelő ellenállás az olvasóban feszültségesést okoz. Melyet, ha ki-bekapcsolgatunk, akkor feszültségingadozás keletkezik. Az ellenállás ki-bekapcsolás pedig az adatoknak megfelelően történik. Pl.: Bináris 0: 0V, bináris 1: 5V.)* küldenek adatokat.

Egy bit átviteléhez 9,44µs-ra van szükség. A passzív kártyák simítókondenzátorokat is tartalmaznak, hogy kisimítsák a tápellátásban lévő ingadozásokat. A kártya alapállapotban *IDLE (tétlen)* állapotban van. Az olvasó periodikusan küld egy *REQA (Request Type A)* parancsot, ami a hatósugarában lévő összes kártyát *READY* állapotba teszi, gyakorlatilag kész állapotba teszi. Aztán a kártya (kártyák) küldenek egy *ATQA (Amswer to Request Type A)* parancsot, ezzel az olvasó tudja, hogy legalább egy kártya van a hatósugarában. Ha több kártya van az olvasó hatókörében, akkor a 14443 A típusra jellemző „bináris kereső fa” *(binary search tree)* algoritmust használj a kártya kiválasztására. Az olvasó küld egy *SELECT (kiválasztás)* parancsot egy *NVB (Number of Valid Bits- Érvényes Bitek Száma)* paraméterrel és egy bitmaszkot. A maszkban lévő bitek száma az *NVB*-től függ. Majd ez a maszk összekomparálódik a kártya saját ID-jével *(ID=Identification Number)*. Ez a komparálás addig ismétlődik, míg egy kártya kiválasztásra nem kerül *(Legalább 64 db érvényes bitnek*

---

[6] ISO/IEC 14443-2: modulációs eljárásra, és kódolásra vonatkozó sémák.
ISO/IEC 14443-3: ütközés elkerülésre *(anti collison)* vonatkozó sémák.
ISO/IEC 14443-4: kommunikációs protokoll leírása.

[7] A Módosított Miller kódolás, vagy más néven Módosított Frekvenciamodulált kódolás a Frekvenciamodulált eljáráson alapszik. A *függelékben található II. ábrán* látható, hogy az FM kódolás minden bitkezdetre és végre betesz egy kezdő és záró impulzust. Ha 0-lát akarunk kódolni, akkor a cella középen üresen marad, ha 1-gyet, akkor nem. A módosított változat *(az ábrán: MFM jelöléssel)* csak annyiban különbözik, hogy elhagyjuk a kezdő és végimpulzusokat.

[8] 3 típus létezik az RFID kártyákból: passzív, szemi-passzív *(semi-passive)* és aktív. A passzív kártyákat az olvasó készülék látja el a kommunikációhoz szükséges energiával. Az aktív kártyák saját áramforrással *(beépített elem)* rendelkeznek, ennek hatására az olvasási távolság a több métert is elérheti. A szemi-passzív kártya működtetése saját áramforrásból származik, kommunikációhoz viszont az olvasó erőterét használja.

[9] Az informatikai rendszerekben ritkán alkalmaznak bináris kódolást, mivel a vevő nem tudja megállapítani, hogy hol vannak a bitkezdetek és a bitvégek. Ehelyett a függelékben található III. *ábrán* látható Manchester-kódolás a használatos. A bináris 1 a bitcella első felében magas, a 0 pedig a második felében magas.

kell lennie!) Ezután a kártya visszatér egy *SAK (Secure Attention Key)* paranccsal és *ACTIVE* állapotba kerül. Ezek után az olvasó és a kártya lebonyolítja egymás között – a megfelelő protokoll szerint – az adatcserét a következő módon: az olvasó először küld egy *RATS (Request Answer to Select)* parancsot, erre válaszul a kártya visszatér egy *ATS (Answer to Select)* paranccsal, ami már tartalmazza a kártya beállításait.
A teljesség kedvéért fontos megemlíteni, hogy az adatkapcsolati réteg kommunikációs protokollja az ISO/IEC 7816-3 T=1 protokollján *(Fél-duplex aszinkron átvitel)* alapul.

3.1. A személyes adatokról

Ha valahol valamilyen ok miatt szükséges adataink egy rendszerben való rögzítése, akkor mindig felmerül az a kérdés, hogy vajon biztonságban vannak-e az adataink, lehetséges-e külső, vagy akár belső személy általi visszaélés? Adataink védelméért, illetve biztonságát az *2011. évi CXII. törvény* szabályozza. Mely hazánkban a többi európai ország adatvédelmi törvényéhez képest nagyobb szigorral szabályoz. A legtöbb kártyán letárolásra kerülnek a személyes adatok. Hazánkban a megszemélyesítés a személyes adatok direkt rögzítésével egy kártya adathordozóján, az adatvédelmi törvény miatt még nem megoldható. Azonban pl. egy ráragasztott matricával már kikerülhető ez a probléma.

4. MIFARE KÁRTYÁK FELÉPÍTÉSE

A világ túlnyomó részén az NXP Mifare kártyákat alkalmazzák. *(Hozzávetőlegesen az összes RFID média 70%-kát fedi le.)* A bérletre leggyakrabban használatos kártya a Mifare Classic 1K és 4K. *(A nem megfelelő biztonság miatt a Classic 1K kártyák Angliában 2016.12.31-ig fokozatosan kivonásra kerülnek.)* A Classic kártyák egy EEPROM-ot és egy rádiófrekvenciás kommunikációt lehetővé tevő interfészt tartalmaznak.

EEPROM felépítése:

MIfare Classic 1K-nál 16db 64 byte-s szektor található, és minden szektor tovább bonható 4db 16 byte-s blokkra. *(Tehát összesen 64 db blokk található egy 1K-s EEPROM-ban.)* Minden szektor utolsó blokkja a tartalmazza a „trailer” részt, mely 2 titkos kulcsot és programozási hozzáféréseket tárol. A függelékben található *I. ábrán* látható a felépítése.

Szektor	Blokk	0 1 2 3 4 5	6 7 8 9	10 11 12 13 14 15	Leírás
15	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 15
	2				DATA
	1				DATA
	0				DATA
14	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 14
	2				DATA
	1				DATA
	0				DATA
1	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 1
	2				DATA
	1				DATA
	0				DATA
0	3	KEY A	ACCESS BITS	KEY B	TRAILER SZEKTOR 0
	2				DATA
	1				DATA
	0				MANUFACTORER BLOCK

1. ábra. Mifare Classic 1K logikai felépítése
Forrás: http://www.cardviser.hu/muszaki_ismerteto.php?id=58; (2011. 03. 14.)

5. TÁMADÁSI MÓDSZEREK

A Mifare kártyák ellen sokféle támadás létezik. A támadások lényege, hogy az adatkapcsolati réteg számára teljesen láthatatlan, mivel a támadások a fizikai rétegre irányulnak.

Az egyik módszer a *lehallgatás*. Egy az erre készített céleszközzel lehallgathatjuk a kártya és az olvasó közötti kommunikációt. Majd pl. az igazi kártya eltulajdonítása után lehetséges az adatok teljes visszafejtése a lehallgatott kommunikációs adatok segítségével.

A következő módszer a *klónozás*, ez akkor jelent gyakorlati problémát, amikor a kártya nincs védve semmiféle titkosítással, továbbá ismert a kártya utasításkészlete. Védelem nélküli, olcsóbb kártyáknál kivitelezhető. Továbbá a klónozás egyszerűen kivédhető a duplikált kártyák figyelésével.

A harmadik módszer az eldobható RFID kártyáknál jelentkezhet, melynél a risszul tervezett rendszer nem figyeli a Lock bit-ek letiltását. Ezzel lehetővé teszi a kártya memóriaterületére való írást. Ezzel pl. jogtalanul újra felhasználhatunk egy kártyát.

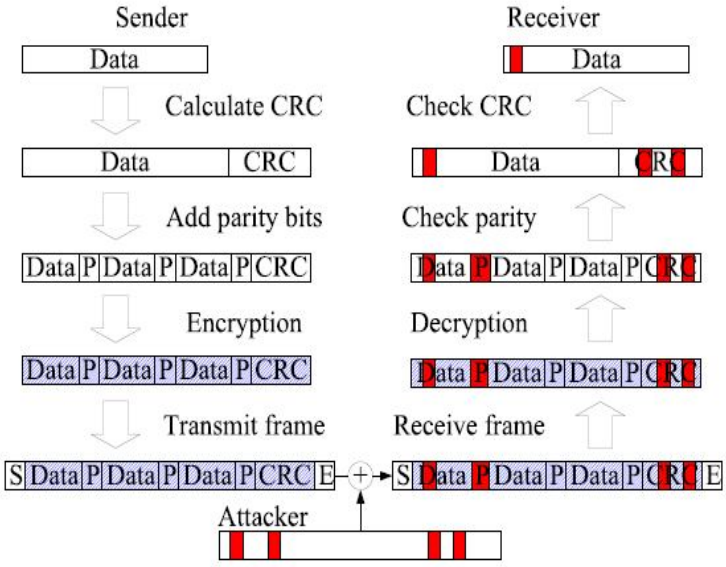
A negyedik megoldás egy hardware-es törési lehetőség a *reverse engineering*. Ha eltulajdonítottunk egy kártyát, és a tervezők nem figyelnek a kártya hardware-es védelmére, akkor visszafejthető a chip hardware-es felépítése, utasításkészlete, stb.

Végül a legveszélyesebbnek vélt módszer a *man in the middle (ember a középpontban, vagy ismertebb nevén közbeékelődéses támadás),* amelyen belül két változatot is meg tudunk különböztetni: az aktív és a passzív módszer. Az aktív módszerrel az áldozat kártyáján változtatásokat is végzünk, passzívnál nem. Talán ehhez a törési formához kell a legkisebb anyagi befektetetés *(100 angol fontból kihozható céleszközt készítettek már 2005-ben)*, és az, hogy a támadó hogyan vitelezi ki csak a kreativitásától, és szakmai ismereteitől függ. A lehallgatástól annyiban tér el, hogy a lehallgatott anyag azonnal felhasználásra kerül. Ehhez két célszerkezet szükséges: egy eredeti kártyaolvasó *(Pl. egy nyílt forráskódú OpenPCD olvasó.)*, és egy Ghost kártyát *(Ez egy eredeti RFID kártya, azzal a különbséggel, hogy számítógéphez csatlakoztatható és programozható.)*. A Ghost kártya az eredeti terminállal felveszi a kapcsolatot, majd továbbítja a terminál által küldött parancsokat a számítógépnek. A számítógép a parancsokat továbbítja az OpenPCD-nek, majd az OpenPCD az eredeti kártyának. Majd visszafelé is lefolytatódik ez a kommunikáció. Az olvasó és a terminál gyakorlatilag azt érzékeli, hogy egymással kommunikálnak, és nincs „középen senki”. Ráadásul nem érdekli a támadót, hogy DES vagy AES kódolással titkosították a kártyát, hiszen megvan számunkra minden kellő információ. Tehát ezzel gyakorlatilag megszereztünk minden adatot, ahhoz hogy egy kis időre „kölcsön vegyük” az áldozat kártyáját. Ez egy bérletnél nem is lenne gond, de ahol a bérlet funkció mellett elektronikus pénztárca funkció is megtalálható, és ezen az elektronikus számlán pénz is található, akkor komoly bevétele lehet a támadónak egy ilyen támadás lefolytatása után. Végezetül az áldozat semmit sem vesz észre a támadás alatt.

Azt fontos megjegyezni, hogy egy átlagos kártya maximális leolvasási távolsága nem haladja meg az 1cm-t az alkalmazott kis hatótávolságú antennája miatt. Ezt azzal ki lehet küszöbölni, hogy létrehozunk egy loop antennát, melyet akár egy teniszütőnek is lehet alkalmazni, oly módon hogy a loop antennával teniszütőformát alakítunk ki, és betesszük egy teniszütő tokba. *(Fontos, hogy a terminállal kommunikáló céleszköznek közel kell lennie az olvasó terminálhoz.)* Visszatérve a loop antennára, segítségével az átjátszási távolság a többi eszköz felé akár 50m-ig is könnyedén kitolható. A lényeg, hogy rövid ideig folyamatos kapcsoltban legyünk a támadott kártyájával.

Többféle kivitelezési mód is létezhet. Az egyik módszer, az esetleges csaló kereskedőkön alapszik. Pl. ha egy kereskedő elhelyez egy hamis kártya feltöltő állomást az üzleténél, akkor plusz bevétele szárazhat abból, hogy a csaló automata csak szelektíven továbbítja a bevételről

szóló adatokat tömegközlekedési társaságnak. A másik, ezen alapuló módszer az, hogy egy szintén csaló kereskedő rejtve elhelyez egy kicsi loop antennát a terminál kártyaolvasójához közel. Kiszemel egy áldozatot, aki frissen töltötte fel a kártyáját, és belépéskor a kereskedő képes megtámadni az áldozat kártyáját, és lecsípni belőle valamekkora összeget. A dupla transzakció *(a törvényes belépésért, és a csalásért)* időben nem észrevehető. A nem túl nagy lecsípett összeg pedig általában nem tűnik fel senkinek. Ez ellen a kártyafeltöltők és a beléptető terminálok együttes figyelhetősége lenne a megfelelő ellenszer. A második módszer azon alapszik, hogy van egy éves bérletünk, és a rendszer nem figyeli a duplikátumokat. Ha csak helyileg figyeli a duplikátumokat, akkor a klónkártyákat felhasználóknak más útvonalon kell közlekedniük. A korábban írottak szerint itt le kell figyelni a rádiófrekvenciás kommunikációt a kártya és a terminál között. Az adatokat felhasználva, pedig létrehozhatunk több virtuális klónkártyát. A kártyákat szét lehet osztani az ismerősök között, azzal a megkötéssel, hogy senki ne menjen ugyanazon a kapun be. Végül a harmadik módszer a Mifare Classic nem megfelelő hitelesítésen, illetve titkosításon alapszik. A man in the middle módszerrel a támadó saját kártyájára több pénzt tölthet fel, mint amennyit befizetett az automatába. A lényeg az, ami a *2. ábrán* is látható, hogy a támadó céleszközökkel bele képes nyúlni a feltöltő terminál által küldött adatkeretbe, azzal meghamisítva a kártya által vett adatkeretet. Természetesen ennél több lehetőség is nyílhat a támadó számára, és nem csak a tömegközlekedés nyújtotta területeken.



2. ábra [1]

E technikák ellen a distance bounding protokoll (távolság korlátozás) használata, illetve a time relay figyelése adhat megfelelő védelmet. (time relay= késés Egy végrehajtott támadás kb 20µs-os késleltetést vitt be a rendszerbe. Csak hasonlításképpen a Frame Waitng Time, azaz a megengedett időtúllépés az ISO/IEC 14443-4 szerint ez FWT=300-tól 5s-ig változhat.) További megoldás lehet egy ultrahangos érzékelő elhelyezése, mely egy beállított távolságlimit után megszakítja a kommunikációt és jelez. A működés azon alapszik, hogy a hangsebesség alacsonyabb a fénysebességnél. Az eszközök Faraday kalickába zárása is megoldást nyújthat a káros rádiófrekvenciás lehallgatások ellen.

6. ÖSSZEGZÉS

Napjainkban a bűnözés nagy része áttevődött a virtuális világba, tehát a"tudós" bűnözők nagy része nem az utcán, szemtől szembe támad a kiszemelt áldozatra, hanem azt a modern információs technológiának köszönhetően a virtuális téren keresztül teszi. Az emberi tehetséget rosszra felhasználók sajnálatos módon már a nagybiztonságú, nyílt forráskódú memóriakártyák feltörésére is képesek lehetnek. Szerencsére a másik oldalon is léteznek leleményes szakemberek, akik azon dolgoznak, hogy optimális védelmet építsenek ki a bűnözők ellen. Erre jó példa a mikroprocesszorral rendelkező intelligens kártya, a smart card, melynek ismertetése egy másik cikk témája lehet.

Felhasznált irodalom

[1] G.P. Hanckea, K.E. Mayesa, K. Markantonakisa, Confidence in Smart: Token Proximity: Relay Attacks Revisited, ISG Smart Card Centre Royal Holloway, University of London Egham TW20 0EX, UK, 2009

[2] Wouter Teepe: Making the Best of Mifare Classic Update, Raunbunk University Nijmegen, 2008

[3] Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia: A Practical Attack on the MIFARE Classic, Institute for Computing and Information Sciences, Radboud University Nijmegen, 2008

[4] Gerhard Hancke: A Practical Relay Attack on ISO 14443 Proximity Cards, University of Cambridge, Computer Laboratory JJ Thomson Avenue, Cambridge, CB3 0FD, UK, 2005

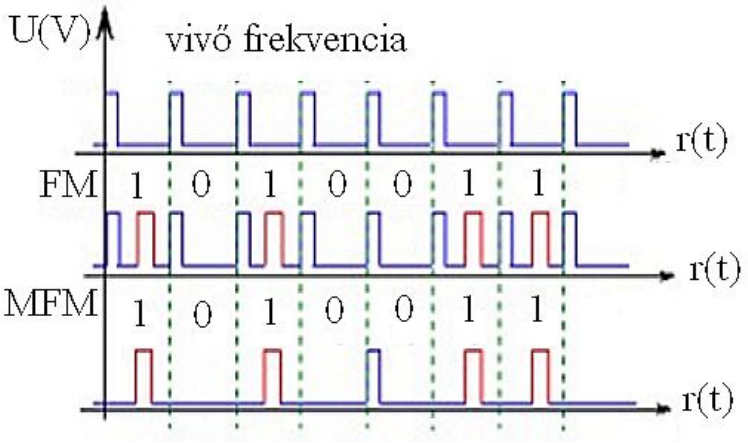
[5] ISO/IEC 14443-4:2008 Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol, 2008.06.04.

[6] ISO/IEC 7816-1:2011 Identification cards -- Integrated circuit cards -- Part 1: Cards with contacts -- Physical characteristics, 2011.01.31.

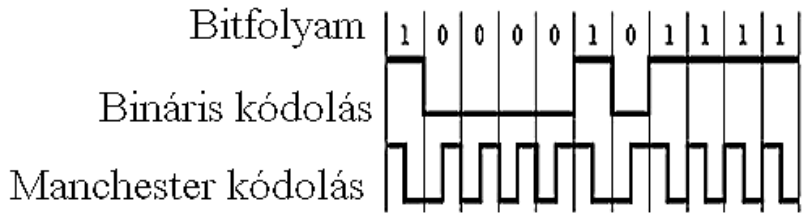
[7] i.sz.: http://vili.pmmf.hu/jegyzet/diplom/1997/lauko/kodok.htm; (2011. 09. 13.)

[8] i.sz.: http://www.remenyikzs.sulinet.hu/segedlet/addatar/adattar.html; (2011. 03. 14.)

Függelék



I. ábra. FM és MFM kódolás [1]



II. ábra. Manchester kódolás
Forrás: http://vili.pmmf.hu/jegyzet/diplom/1997/lauko/kodok.htm; (2011. 09. 13.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Kovács Zoltán
zkovacs@nbsz.gov.hu

CLOUD SECURITY IN TERMS OF THE LAW ENFORCEMENT AGENCIES

Absztrakt/Abstract

A felhő alapú rendszerek költségcsökkentő és hatékonyságnövelő tulajdonságaik miatt egyre jobban elterjednek. Ez a tény több szempontból is új kihívások elé állítja a rendvédelmi szerveket. Egyrészről a felhő alapú rendszerek használata elkerülhetetlennek tűnik a rendvédelmi szervek számára, ezért mint (leendő) felhasználóknak tisztában kell lenniük azok biztonsági kockázataival, kihívásaival. Másrészről ezeknél a rendszereknél is biztosítani kell a törvényes ellenőrzést, amely szintén új fajta gondolkodásmódot és megoldásokat igényel a rendvédelmi szervektől és a szolgáltatóktól egyaránt. A cikk a rendvédelmi szervek sajátos – és a fent említett kettős szerepe – szempontjából csoportosítja a felhő alapú rendszerek biztonsági kérdéseit.

Due to its cost reducing and efficiency increasing features cloud computing is becoming more and more widespread. This fact poses new challenges to the law enforcement agencies in several aspects. On the one hand, application of cloud computing seems inevitable for the law enforcement agencies, thus as (future) users should be aware of their security risks and challenges. On the other hand, it is imperative to ensure lawful monitoring, which requires new approaches and solutions from both the law enforcement agencies and the service providers. This article describes the challenges of cloud computing security issues, grouping them in terms of the special – and the aforementioned dual role – of the law enforcement agencies.

Kulcsszavak/Keywords: *felhő alapú informatika, felhő alapú rendszerek biztonsága, törvényes ellenőrzés ~ cloud computing, cloud security, lawful monitoring*

1. INTRODUCTION

The law enforcement agencies have to face new challenges by the spread of cloud computing systems. Due to the efficiency and the lower expenditure, reserving their high safety requirements these organizations will sooner or later apply systems like these [1]. However, the greatest challenge of cloud computing, as a recently appeared, rapidly and continuously developing, altering technology is establishing complete security. The traditional IT safety solutions cannot entirely be applied in the cloud, what is more, there are new security risks which require new solutions. In addition, the interests of the users and the cloud providers – due to the expenditures and the responsibility to provide security – might be contrary.

The law enforcement agencies have to be concerned with cloud not only as users, but also as an organisation doing lawful monitoring as well. In this role, besides the technical challenges given by the new technology, the other accentuated problem is that the traditional (communication) provider model is being replaced by a new model, thus the creation of the lawful monitoring requires not only technical, but also new legal solutions and lateral thinking.

What security issues should be considered with in the cloud? What aspects should be examined concerning security? Can the issues which have to be considered during the contracting be defined so that the system used will meet – the sometimes really high - requirements of the law enforcement agencies? This article is searching the answers for these questions, collecting viewpoints published on cloud, complementing and organizing the reasons in a specific way.

2. SECURITY ISSUES – BASICS

The studies, blogs on cloud computing published on the INTERNET, search for answers or try to give definitions, advice in a plenty of ways, sometimes aspiring to completeness, sometimes riving off a very focussed topic related to the security of cloud computing. Like in the definition and categorization of cloud computing the study published by the Information Technology Laboratory of NIST (National Institute of Standards and Technology) under the title „The NIST Definition of Cloud Computing" is regarded widely accepted and quasi-standard, as far as security concerned the same could be written about the „SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING" [3] by Cloud Security Alliance. Accepting the content of this study, in this article the major issues of the security of cloud computing will be reviewed on the basis of this categorisation hereinafter.

In the document, the security aspects are divided into 13 domains, further classified into 2 main parts: governance and operation. The governance part includes mostly strategic, while the operational part discusses tactical security questions. The domains defined by the CSA and their short description can be found in the chart below:

DOMAIN	GUIDANCE DEALING WITH...
Governance and Enterprise Risk Management	The ability of an organization to govern and measure enterprise risk introduced by cloud computing. Items such as legal precedence for agreement breaches, ability of user organizations to adequately assess risk of a cloud provider, responsibility to protect sensitive data when both user and provider may be at fault, and how international boundaries may affect these issues.
Legal Issues: Contracts and Electronic Discovery	Potential legal issues when using cloud computing. Issues touched on in this section include protection requirements for information and computer systems, security breach disclosure laws, regulatory requirements, privacy requirements, international laws, etc.
Compliance and Audit	Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (regulatory, legislative, and otherwise) are discussed here. This domain includes some direction on proving compliance during an audit.
Information Management and Data Security	Managing data that is placed in the cloud. Items surrounding the identification and control of data in the cloud, as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud, are discussed here. Other items, such as who is responsible for data confidentiality, integrity, and availability are mentioned.
Portability and Interoperability	The ability to move data/services from one provider to another, or bring it entirely back in-house. Together with issues surrounding interoperability between providers.

1/a. table. Governance Domains [3]
Source: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; (05/01/12)

DOMAIN	GUIDANCE DEALING WITH...
Traditional Security, Business Continuity and Disaster Recovery	How cloud computing affects the operational processes and procedures currently used to implement security, business continuity, and disaster recovery. The focus is to discuss and examine possible risks of cloud computing, in hopes of increasing dialogue and debate on the overwhelming demand for better enterprise risk management models. Further, the section touches on helping people to identify where cloud computing may assist in diminishing certain security risks, or entails increases in other areas.
Data Center Operations	How to evaluate a provider's data center architecture and operations. This is primarily focused on helping users identify common data center characteristics that could be detrimental to on-going services, as well as characteristics that are fundamental to long-term stability.
Incident Response, Notification and Remediation	Proper and adequate incident detection, response, notification, and remediation. This attempts to address items that should be in place at both provider and user levels to enable proper incident handling and forensics. This domain will help you understand the complexities the cloud brings to your current incident-handling program.
Application Security	Securing application software that is running on or being developed in the cloud. This includes items such as whether it's appropriate to migrate or design an application to run in the cloud, and if so, what type of cloud platform is most appropriate (SaaS, PaaS, or IaaS).
Encryption and Key Management	Identifying proper encryption usage and scalable key management. This section is not prescriptive, but is more informational in discussing why they are needed and identifying issues that arise in use, both for protecting access to resources as well as for protecting data.
Identity and Access Management	Managing identities and leveraging directory services to provide access control.

DOMAIN	GUIDANCE DEALING WITH...
	The focus is on issues encountered when extending an organization's identity into the cloud. This section provides insight into assessing an organization's readiness to conduct cloud-based Identity, Entitlement, and Access Management (IdEA).
Virtualization	The use of virtualization technology in cloud computing. The domain addresses items such as risks associated with multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, etc. This domain focuses on the security issues surrounding system/hardware virtualization, rather than a more general survey of all forms of virtualization.
Security as a Service	Providing third party facilitated security assurance, incident management, compliance attestation, and identity and access oversight. Security as a service is the delegation of detection, remediation, and governance of security infrastructure to a trusted third party with the proper tools and expertise. Users of this service gain the benefit of dedicated expertise and cutting edge technology in the fight to secure and harden sensitive business operations.

1/b. table. Operational Domains [3]
Source: http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; , (05/01/12)

The Cloud Security Alliance^{SM} (CSA) first published the study mentioned above in April 2009, the V3.0 version of which was published in 2011. In the latter one, the concept of Security as a Service (SecaaS) (Chart1, last domain) appeared first. About the purpose of its introduction the authors wrote the followings:

„SecaaS is looking at Enterprise security from the cloud – this is what differentiates it from most of the other work / research on cloud security. Predominantly cloud security discussions have focused on how to migrate to the Cloud and how to ensure Confidentiality, Integrity, Availability and Location are maintained when using the Cloud. SecaaS looks from the other side to secure systems and data in the cloud as well as hybrid and traditional enterprise networks via cloud-based services. These systems may be in the cloud or more traditionally hosted within the customer's premises. An example of this might be the hosted spam and AV filtering. "

In 2011 Security as a Service Working Group of Cloud Security Alliance^{SM} published a study under the title „Defined Categories of Service 2011"[4], which discusses the above-mentioned topics in detail. In accordance with the content of the basic document, the authors differentiate 10 categories within the topic "Security as a Service" as follows:

- Category 1: Identity, (Entitlement,) and Access Management: *„Identity and Access Management (IAM) should provide controls for assured identities and access management."*
- Category 2: Data Loss Prevention: *„Data Loss Prevention is the monitoring, protecting, and verifying the security of data at rest, in motion and in use both in the cloud and on-premises."*
- Category 3: Web Security: *„Web Security is real-time protection offered either on-premise through software/appliance installation or via the cloud by proxying or redirecting web traffic to the cloud provider."*
- Category 4: Email Security: *„Email Security should provide control over inbound and outbound email, thereby protecting the organization from phishing, malicious attachments, enforcing corporate polices such as acceptable use and spam, and providing business continuity options."*
- Category 5: Security Assessments: *„Security assessments are third-party audits of cloud services or assessments of on- premises systems via cloud-provided solutions based on industry standards."*

- Category 6: Intrusion Management: *„Intrusion Management is the process of using pattern recognition to detect and react to statistically unusual events. This may include reconfiguring system components in real time to stop / prevent an intrusion."*
- Category 7: Security Information and Event Management (SIEM): *„Security Information and Event Management (SIEM) systems accept (via push or pull mechanisms) log and event information. This information is then correlated and analyzed to provide real-time reporting and alerting on incidents / events that may require intervention. The logs are likely to be kept in a manner that prevents tampering to enable their use as evidence in any investigations."*
- Category 8: Encryption: *„Encryption is the process of obfuscating/encoding data (usually referred to as plain text) using cryptographic algorithms the product of which is encrypted data (usually referred to as ciphertext)."*
- Category 9: Business Continuity and Disaster Recovery: *„Business Continuity and Disaster Recovery are the measures designed and implemented to ensure operational resiliency in the event of any service interruptions."*
- Category 10: Network Security.: *„Network Security consists of security services that allocate access, distribute, monitor, and protect the underlying resource services. Architecturally, network security provides services that address security controls at the network in aggregate or specifically addressed at the individual network of each underlying resource."*

Besides the short description, all the categories are classified according to their nature (preventative, protective, detective, reactive) and the most relevant pieces of information is described list-like, in a chart form, as follows:

- core functionalities
- optional features
- challenges
- services
- threats addressed
- reference examples
- references / additional resources.

In these two documents, some overlaps can be observed between the given domains in the basic document and in the categories of the domain "Security as a Service" (e.g.: Identity and Access Management, Encryption etc.). These overlaps indicate how novel the security problems of cloud computing are, and there are not completely accurate circumscriptions, definitions and standards. The participants and stakeholders of this industry – including CSA, ETSI and ITU – are working on it.

3. SECURITY ISSUES – IN TERMS OF THE LAW ENFORCEMENT AGENCIES

In the aforesaid documents the CSA discusses the security issues of cloud computing focussing on business organizations. For the law enforcement agencies – owing to their special status – these documents are worth applying for analysis, but classifying differently, sometimes complementing and modifying the content. The analysis should be carried out along the four dimensions below:

The role of the law enforcement agencies:

- user,
- executor of lawful monitoring.

- Deployment Models:
  - Private cloud,
  - Community cloud,
  - Public cloud,
  - Hybrid cloud.
- Service models:
  - Cloud Software as a Service (SaaS),
  - Cloud Platform as a Service (PaaS),
  - Cloud Infrastructure as a Service (IaaS).
- Security questions for analysing:
  - operational reliability, operational safety,
  - data security,
  - other (legal, physical, etc.) security,
  - lawful monitoring.

3.1. The role of the law enforcement agnecies:

The role of law enforcement agencies can be twofold. On the one hand as a user, they can satisfy their own demands according to their – sometimes really high – security requirements, on the other hand they have to execute the tasks of lawful monitoring, according to acts and laws.

Because of the double role, the security issues should be analysed from a dual perspective. For instance, the availability and the interoperability are very important for the users, but not so relevant for the executors of lawful monitoring. On the other hand, retaining the users activity logs might be more significant for the law enforcement agencies being in the role of executor of lawful monitoring, than as users.

During the analysis it must be considered that in certain cases the enforcement of the lawful monitoring's requirements is contrary to the interests of both the provider and the user (it is the providers' responsibility to cover the costs of installing and maintaining it, while the reason why the users decide to use the cloud is to avoid lawful monitoring).

3.2. Deployment models:

The definition of deployment models can be found in several articles (e.g.: in [1], [2]), thus this article does not discuss it. For reasons of simplification it can be assumed that the law enforcement agencies as users will use a private cloud, while they will focus on public clouds regarding the lawful monitoring. In this case the analysis will be simplified to two dimensions, thus it is worth working out templates which could be applied by many law enforcement agencies. (Certainly, in other cases considering the peculiarities of the given role and the deployment model, the content of the template has to be reconsidered and the questions of security must be re-analysed.)

3.3. Service models:

The definition of service models can be found in many articles (e.g.: in [1], [2]), thus this article does not deal with it.

3.4. Security questions for analysing:

As was mentioned at the beginning of this article, the studies, blogs on cloud computing published on the Internet, search for answers or try to give definitions, advice in a plenty of ways, sometimes aspiring to completeness, sometimes riving off a very focussed topic related to the security of cloud computing, or draw attention to a less known security issue.[5-15][21-22] The more significant participants of this market publish different studies focussing on

specific security issues with the unconcealed aim to offer solutions for these issues with their own products.[16-20]

Based on the CSA documents outlined in the previous chapter, and applying the aforementioned articles and blogs – in a different way, however, - it is advisable to classify the security issues to be considered into four main groups:

- 3.4.1. operational reliability, operational safety
- 3.4.2. data security
- 3.4.3. other (legal, physical, etc.) security
- 3.4.4 lawful monitoring.

3.4.1. Operational reliability, operational safety

The questions of operational reliability as far as cloud computing concerned are considerably analogous with that of the traditional IT systems. It concludes the features relating to the reliable functionality and operation in normal circumstances. For instance accessing the service with the devices defined in the contract (e.g. tablet PCs with Android operational system), from a particular place (anywhere where the Internet connection is available) with defined availability (e.g. 95%, with the loss of service is not longer than 30 minutes), in addition the operational reliability includes the backup of our data, redundant storage and disaster recovery as well.

The questions of operational reliability can be managed purely in a technical way, where the interests of the providers and the users concur (the providers intend to provide, while the users intend to receive a reliable service). The extent of the safe service is merely a matter of money and agreement. (About the possibilities of the users concerning the contract see the chapter on "Other (Legal, Physical, etc.) Security".)

Regarding the operational reliability field, the separation of responsibilities seems to be obvious, basically it is the providers that take all responsibilities, regardless of the service models (SaaS, PaaS, Iaas).

The applied standards and solutions concerning the traditional IT provide a perfect starting point for the analysis of the operational reliability issues of cloud computing. Here the undermentioned questions are to be examined:

- From CSA's governance domains [3]:
  - Portability and Interoperability
  - Compliance
- From CSA's operational domains:
  - Business continuity [3][4]
  - Disaster recovery [3][4] [7]
  - Data Center Operations [3]
- Others:
  - Availability [5][12] or Reliability and liability [22]: availability of your data in the cloud in normal way or in a redundant and highly available way, expect the cloud to be a reliable resources.
  - Redundancy (include: redundant storage) [23]: redundancy supports high availability for the application layer, and must be built-in across the infrastructure and associated tools.
  - Access and usage restrictions [22]: access and use the cloud where and when you wish.
  - Risk Mitigation Plan [21]: This plan should include documentation of risk, responses to those risks, and education and training.
  - Data format [10]: In which kind of format of data have to transfer your data into the cloud (provider) and can you get back your data from the provider.

3.4.2. Information Management and Data Security

All the factors emerging with reference to the safe access to the users' data (management, application etc.), and the prevention of unauthorized access can be regarded as a question of information management and data security (hereafter data security), for instance the identity and access management, the use of encryption and the protecting against phising. Some of them are already available in connection with the traditional IT systems, or can easily be implemented to the cloud (e.g. antivirus protection), the others require completely new solutions (e.g. data segregation, protection against cross-VM side-channel attacks [11]). Some of the data security issues can easily be solved (e.g. shutting down unnecessary and vulnerable applications) others require technically complex, or even legal solutions (so that the providers – including their system administrators – can not have access to our data [10][22].

The data security issues can be solved in technical, legal and administrative ways, however, some of the elements can not be solved only in a technical way, or can be solved with unreal large expenditure (for example the questions of prevention of the cloud provider espionage [12] or insecure or incomplete data deletion [14].)

Concerning the data security issues, the providers and the users might have diverse interests. The primary interest of the providers is a reliable service, the defence of the users' data is subsidiary. Due to the permanent urge of development it means extra and considerably high expenses which are hard to devolve entirely to the user, at the same time the data security is definitely in the users' own interest.

The responsibilities are distributed between the users and the providers and the degree of distribution significantly depends on the service model. The responsibilities of the users are minor in the SaaS model, but they are considerable in the IaaS model. The issues to be examined are as follows.

- From CSA's governance domains [3]:
  - Information Management and Data Security (ezen belül főleg Data Security).
- From CSA's operational domains:
  - Incident Response, Notification and Remediation [3]
  - Application Security [3]
  - Encryption and Key Management [3] [4]
  - Identity and Access Management [3] [4]
  - Virtualization [3]
  - Security as a Service [3] [4]
  - Data Loss Prevention
  - Web Security
  - Email Security
  - Intrusion Management [3] [4] [6]
  - Security Information and Event Management (SIEM)
  - Network Security
- Others:
  - The documents of CSA entirely cover the data security issues.

The questions of data security should be analysed through the life cycle of the data, which is illustrated by Figure 1.

1. figure. Data lifecycle
Source: https://securosis.com/blog/data-security-lifecycle-2.0; (05/01/12)

In terms of security the 6 phases of the data lifecycle can be divided into 2 main groups concerning security: phases with and without data movement.

Phases with data movement:

- create
- use
- share
- destroy

Phases without data movement:

- store
- archive

(Note that in the case of cloud computing, any kind of active operation done by the users will be associated with data movement.)

This classification is to be done to separate the responsibilities of the users and the providers in the different service models, (within a model the users have greater responsibilities in operations including data movement than in operations without data movement), which can help make templates mentioned in the deployment models.

3.4.3. Other (legal, physical, etc.) security

This category includes all the security issues which can not be managed in a technical way, or even a third party can be involved (e.g. audit). The legal guarantees (primarily contractual, or regulated by the law) which can solve the particular issues in an unambiguous way, including the questions emerging about reliability and data security issues, as well as the physical defence of data centres are classified here.

The questions belonging to this category can be solved only in legal ways (the legal issues are given, but the physical security or the audit, which require involving a third party, can be influenced by the users only through legal ways).

In this category, the interests of the providers and the users differ in each case. The influence of the users on the questions belonging to this category, e.g. the content of the contract, can vary between the extremes (e.g. while in (a public) SaaS model this can be the approval or disapproval of a contract (including all conditions) written by the providers, in a (private) IaaS solution the content of the contract and the other conditions can be defined in a negotiation directly between the providers and the users).

It is where the separation of responsibilities is probably the most unambiguous, the responsibilities of the users extend to ascertain each relevant question in the contract, including the supervision of the written requirements as well. The physical, technical

implementation written in the contract belongs to the responsibilities of the providers. The questions to be analysed are as follows:

- From CSA's governance domains [3]:
  - Governance and Enterprise Risk Management
  - Legal Issues: Contracts and Electronic Discovery
  - Audit
- From CSA's operational domains:
  - Traditional Security [3]
  - Security Assessments [4]
- Others:
  - Long-term viability [7]: you must be sure your data will remain available even after your cloud computing provider go bankrupt or get acquired and swallowed up by a larger company.
  - Access logs and other statistics ownership [10]: in the contract it has to be regularized, what the providers are allowed to do with the logs and other statistical information – collected by themselves – because sensitive information can be extracted from this logs.
  - Cloud provider espionage [12]: in the contract, the access to the user's data by the provider (including its administrators and other professionals) has to be regularized so that it will extend over not only the random and (sometimes inevitable) normal access cases (which may be necessary for the providers' work), but also the theft of company proprietary information by the cloud provider.
  - Transitive nature [12]: the cloud provider might use subcontractors, the cloud user has not contract with them. These issues should also be regularized.
  - Insecure or incomplete data deletion [14]: the user's data should really be deleted (if it is the users' request), so that they can not be recovered, even from back-up.

3.4.4. Lawful Monitoring

While the previously examined security issues are more relevant for the law enforcement agencies as users, and less relevant as the executors of lawful monitoring, in this issue, it is just the opposite. This group includes those forms of monitoring which have already been developed and accepted in the traditional communication networks (e.g. lawful interception), and those that have been developed specifically for IT systems (e.g. computer forensics).

The issues belonging to lawful monitoring can be resolved in technical and legal ways, but at the moment these are the most complicated questions. On the one hand, the legal relationship has been set up between the providers and the executors of lawful monitoring (not between the providers and the users, as in the cases of other security issues), and this relationship is usually based on legal obligations. While concerning the communication networks there is an evolvelved, widely accepted lawful monitoring based on similar laws in democratic states, as regards cloud computing it is different. The lack of currently existing legal regulation might cause problems concerning lawful monitoring, or even it might prohibit it. For this reason, you can not talk about such sophisticated monitoring systems, like the ones that are available as concerns telephone systems.

In this category, the interests of the providers and the users are almost the same, but contrary to that of law the enforcement agency which executes the tasks of lawful monitoring, as it was mentioned concerning the roles of the law enforcement agencies. There are only a

few exceptions (e.g. applying devices which can be suitable to confirm or exclude whether the data stored in the cloud was generated originally by a specific user or they were manipulated).

The responsibilities are clear, as long as there are statutory requirements, or can be made clear, if in the lack of regulation, the law enforcement agency and the provider do a contract.

As concerns lawful monitoring the issues to be analysed are as follows:

- data retention
- lawful interception
- forensics tools.

As the concept of Security as a Service was introduced in the above-mentioned documents of CSA, the concept of Lawful Monitoring as a Service (LMaaS) (or something like that) might be introduced. If this concept – like the other issues – can be standardised, the providers can provide the required information to the law enforcement agencies as a service, regardless of the nationalities of the participants, the physical location of the data centres and other technical devices, and the questions, when and which country's legal system should be followed.

4. CONCLUSIONS

This article has reviewed the security *issues* of cloud computing, and then established a unique, essential classification in terms of the law enforcement agencies. From the „Service models – Deployment models – The role of law enforcement agencies – Security questions for analysing" four-dimensional space the latter two have been examined in detail. The chapter "Security issues to be analysed" sets up a new classification where it introduces what is meant by operational reliability/operational safety, data security, other (legal, physical, etc.) security and lawful monitoring, the way they can be solved (technically, legally), how the previously mentioned questions can be classified into the newly set up category, as well as how the interests of the parties relate to each other.

As a conclusion, the law enforcement agencies are able to set up strong security requirements for cloud as a result of the more and more clear security standards, with the proviso that the continuous monitoring and upgrade of the security requirements and solutions are crucial due to the technical development and the recently appearing threats. It is not so easy for the executors of lawful monitoring, in these cases further legal and technical solutions should be searched and found, during a corresponding standardising process, which all the questions (thus security questions) of cloud computing go through.

Conclusions drawn from this article:

- Concerning lawful monitoring the concept of Lawful Monitoring as a Service (LMaaS) (or something like that) should be introduced and standardised.
- Templates are to be worked out based on the most frequently used cases (law enforcement agencies as users use private cloud, as executors of lawful monitoring focus on public cloud), and can be applied by law enforcement agencies freely, so that the agencies will not have to work out comprehensive requirements.

References

[1] Kovács Zoltán: Felhő alapú informatikai rendszerek potenciális alkalmazhatósága a rendvédelmi szerveknél – Hadmérnök VI. Évfolyam 4. szám - 2011. december

[2] Peter Mell and Tim Grance: The NIST Definition of Cloud Computing Version 15, 10-7-09; http://www.nist.gov/itl/cloud/index.cfm; (2011. 10. 21.)

[3] SECURITY GUIDANCE FOR CRITICAL AREAS OF FOCUS IN CLOUD COMPUTING V3.0 http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf; (2012. 01. 05.)

[4] Defined Categories of Service 2011 https://cloudsecurityalliance.org/wp-content/uploads/2011/09/SecaaS_V1_0.pdf; (2012. 01. 05)

[5] Ariel Silverstone: Clear Metrics for Cloud Security? Yes, Seriously http://www.csoonline.com/article/507823/clear-metrics-for-cloud-security-yes-seriously?page=1; (2012. 01. 02.)

[6] [6] Phil Cox: Intrusion detection in a cloud computing environment http://searchcloudcomputing.techtarget.com/tip/Intrusion-detection-in-a-cloud-computing-environment; (2012. 01. 02.)

[7] Jon Brodkin: Gartner: Seven cloud-computing security risks http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853?page=0,0; (2012. 01. 02.)

[8] Phil Cox: Securing data in the cloud http://searchcloudcomputing.techtarget.com/tip/Securing-data-in-the-cloud; (2012. 01. 02.)

[9] Francoise Gilbert: Ten key provisions in cloud computing contracts http://searchcloudsecurity.techtarget.com/tip/Ten-key-provisions-in-cloud-computing-contracts; (2012. 01. 02.)

[10] Joseph Foran: Ten questions to ask when storing data in the cloud http://searchcloudcomputing.techtarget.com/tip/Ten-questions-to-ask-when-storing-data-in-the-cloud; (2012. 01. 02.)

[11] Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage: Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf ; (2011. 11. 05.)

[12] Richard Chow, Philippe Golle, Markus Jakobsson, Elaine Shi, Jessica Staddon , Ryusuke Masuoka, Jesus Molina : Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control http://www.parc.com/publication/2335/controlling-data-in-the-cloud.html; (2011. 11. 05.)

[13] Yanpei Chen, Vern Paxson, Randy H. Katz: What's New About Cloud Computing Security? www.eecs.berkeley.edu/Pubs/TechRpts/2010/EECS-2010-5.pdf; (2011. 11. 05.)

[14] DANISH JAMIL, HASSAN ZAKI: CLOUD COMPUTING SECURITY www.ijest.info/docs/IJEST11-03-04-129.pdf; (2011. 11. 05.)

[15] http://blogs.forrester.com/security_and_risk/2009/11/cloud-security-front-and-center.html; (2011. 10. 23.)

[16] Virtualization and Cloud Computing: Security Threats To Evolving Data Centers (Trend Micro) http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/final_cloud_virt_report.pdf; (2011. 11. 05.)

[17] Securing Microsoft's Cloud Infrastructure
http://www.globalfoundationservices.com/security/; (2011. 11. 05.)

[18] Intel's Vision of the Ongoing Shift to Cloud Computing
http://charltonb.typepad.com/papers/Cloud Vision.pdf; (2011. 12. 03.)

[19] Virtualization and Cloud Computing: Security Best Practice (Trend Micro)
http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/final_cloud_virt_best_practice.pdf; (2011. 11. 05.)

[20] Axel Buecker , Koos Lodewijkx , Harold Moss , Kevin Skapinetz , Michael Waidner : Cloud Security Guidance (IBM Recommendations for the Implementation of Cloud Security) Redpaper
http://www.redbooks.ibm.com/redpieces/abstracts/redp4614.html?Open&pdfbookmark; (2012. 01. 02.)

[21] Chris Preimesberger: Cloud Computing: Cloud Computing Security: 10 Ways to Enforce It
http://www.eweek.com/c/a/Cloud-Computing/Cloud-Computing-Security-10-Ways-to-Enforce-It-292589/; (2011. 11. 05.)

[22] Paul T. Jaeger, Jimmy Lin, Justin M. Grimes: Cloud Computing and Information Policy: Computing in a Policy Cloud?
http://www.tandfonline.com/doi/abs/10.1080/19331680802425479; (2011. 11. 05.)

[23] http://blogs.sungard.com/as_cloud/tag/cloud-computing-redundancy/; (2012.01.24.)

[24] https://securosis.com/blog/data-security-lifecycle-2.0; (2012. 01. 05.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Kuris Zoltán
zoltan.kuris@bm.gov.hu

THE PROTECTION OF CLASSIFIED INFORMATION, COMPLEX SUBSYSTEMS

Absztrakt/Abstract

Jelen cikkben a szerző ismerteti a hazai nemzeti és külföldi minősített adatokat kezelő komplex rendszer személyi, fizikai, adminisztratív és elektronikai védelemre vonatkozó követelményeket, a megvalósításukkal kapcsolatos dilemmákat, valamint javaslatokat fogalmaz meg a még nem szabályozott területein elveiket, módszereiket és eszközeiket illetően.
A minősített adatokat kezelő rendszerekben kezelt minősített adat bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása komplex védelmi intézkedéseket igényel a rendszer teljes életciklusában. Ezen intézkedések csak akkor lehetnek kellően hatékonyak, költségek szempontjából is optimalizáltak, ha azokat a biztonsági kockázatokkal arányosan tervezik és implementálják.

In this article the author demonstrates the personnel, physical, administrative and electronic protection requirements of national and international classified data handelingv complex systems, and, the design-related dilemmas about their implementation, in additon draws up recommendations about their principles, methods and instruments for the unregulated areas.
The confidentiality, integrity and availability, of classified information that is handled in systems dealing with classified information, require complex protective measures during the entire life-cycle of the system. Such measures should be enough efficient and cost-efficient if they are designed and implemented regarding of the security risks.

Kulcsszavak/Keywords: *minősített adatok, zárt terület, kommunikáció biztonság, bizalmas adat, információ biztonság, nemzeti minősített ada, szükséges tudni, biztonsági terület, korlátozott terjesztésű adat ~ classified information, closed area, communications intelligence, confidential, facility, information security, national security information, need-to-know, restricted area, restricted data*

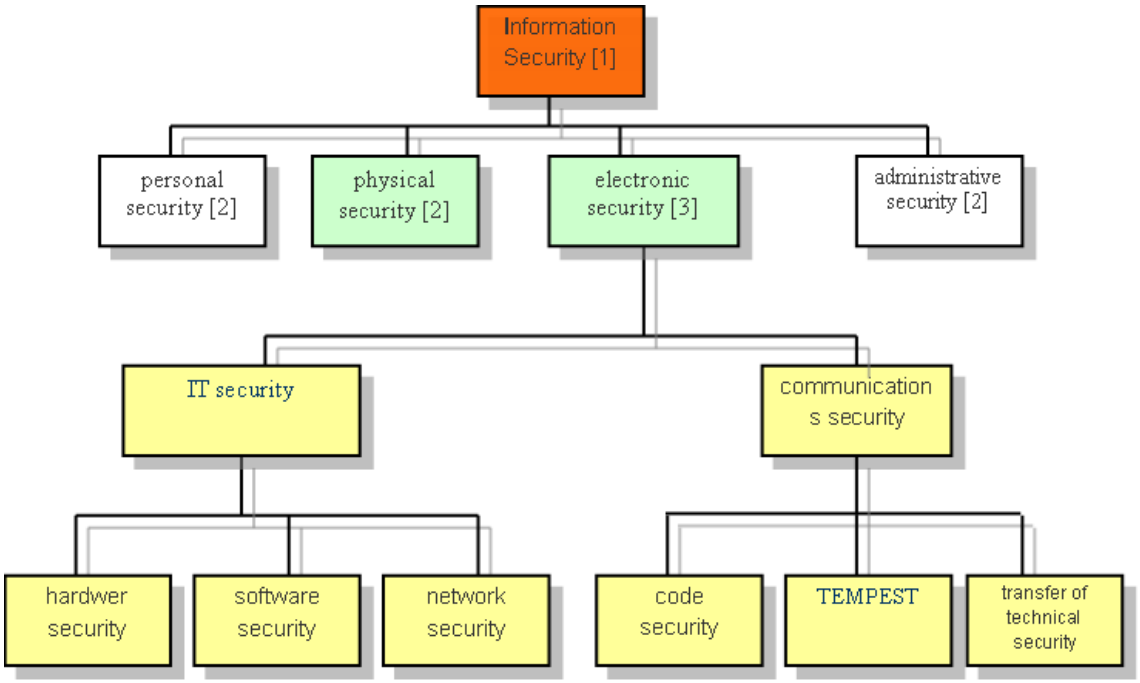
1. INTRODUCTION

The statutory rules of the government decree [1].

The government dercree of safety includes the following areas of expertise [2; 3]:

- personal security
- physical security
- administrative security
- electronic security

The safety provider secures the operation of the system in all area. The security system is made up of subsystems:



1. figure. the comlex information security systems

2. PERSONAL SAFETY (USER AUTHORIZATION)

A security clearance is a privilege, not a right. When the user accepts the privilege of access to classified information, someone also accepts the responsibilities of this privilege. The user's responsibility is the classified information protecting, which means a LIFELONG obligation. It continues afterwards someone no longer has an active security clearance. The Nondisclosure Agreement is signed when accepting your clearance, which is a legally binding agreement between the user and the state. If someone do not comply with procedure of classified information, the agremment's legal sanctions are executed beacause of breaching this contract. The intentional violation - with purpose to enrichment- may be prosecuted. This agreement assign the legal right of any payments to the state Government, royalties or other benefits, which someone could receive as a result of unauthorized disclosure of classified information.The signed Nondisclosure Agreement is the only form to hold on file long after you retire.

The personnel security is an application of measures to ensure that certified data is only known by individuals who has [4]:

A need-to-know, been security cleared to the relevant level, where appropriate, and been briefed on their responsibilities.

The personnel security clearance procedures shall be designed to determine the individual's loyalty, trustworthiness and reliability.

[1]That sums it up. The individual – not our foreign adversaries or competitors – is the principal source of the problem, but the person can also become the solution. Anybody who holds a security clearance is the first line of defense against espionage and other loss of sensitive information. If everybody fulfill our responsibilities, we have the power to protect our national security and economic interests.

3. NEED-TO-KNOW

Need-to-know is difficult to implement as it conflicts with our natural desire to be friendly and helpful. It also requires a level of personal responsibility that many of us find difficult to accept. The importance of limiting sensitive information is who have a need to know is underscored. every time a trusted insider is found to have betrayed that trust. The security clearance does not give approved access to all classified information. It gives access only to that Information at the same or lower level of classification which the level of the clearance granted; AND that you have a "need-to-know" in order to perform your work. Need-to-know is one of the most fundamental security principles. The practice of need-to-know limits the damage that can be done by a trusted insider who has ill-will. The failures of the need-to-know principle implementing have contributed greatly the damage caused by a number of recent espionage cases.

Need-to-know imposes a dual responsibility on all the other authorized holders of classified information. When doing your job, you are expected to limit your requests for information to that which you have a genuine need-to-know. Under some circumstances, the user may be expected to explain and justify your need-to-know when asking others for information. Conversely, the user has to ensure that anyone, - who get the classified information - has a legitimate need to know that information. The user liable for asking the other person about the sufficient information to make a well-founded decision about their need-to-know. On the other hand the recipient person is obliged to justify their need-to-know. The user is expected to refrain from discussing classified information in hallways, cafeterias, elevators, rest rooms or smoking areas where the discussion may be overheard by persons who do not has a need-to-know the subject of conversation. The user is also obliged to report to the user's security office any co-worker who repeatedly violates the need-to-know principle.

4. CERTIFICATION PROCESS

The original classification is the initial determination which define the requires of protection.

Only the Government officials, whom this authority has been delegated in writing and who have been trained in classification requirements, have the authority for original classification. Original classification authorities issue security classification guides, that others use in making derivative classification decisions. Most government employees and contractors make derivative classification decisions. Derivative classification is the act of classifying a specific item of information or material on the basis of an original classification decision by an authorized original classification authority. The source of authority for derivative

[1] Pogo, a popular cartoon character from the 1960s, coined an oft-quoted phrase:
"We have met the enemy, and he is us."

classification ordinarily consists of a previously classified document or a classification guide issued by an original classification authority.

5. CLASSIFICATION LEVELS

The competent authorities shall ensure the appropriately classification, clearly identifcation (as classified information) and the classification level for only as long as necessary. Classified information can not be downgraded or declassified nor shall any be modified or removed without the prior written consent of the originator [4].

Information that must be controlled to protect the national security, who is assigned one of four levels of classification, as follows:

- TOP SECRET information is an information which is disclosed without authorization, could reasonably be expected to cause exceptionally grave damage to the national security.
- SECRET information is an information which is disclosed without authorization, it could reasonably be expected to cause serious damage to the national security.
- CONFIDENTIAL information is an information which is disclosed without authorization, it could reasonably be expected to cause damage to the national security.
- RESTRICTED information is an information which is disclosed without authorization, it could be disadvantageous to the interests of the national security.

Any approved holder of classified information - who believes the information is classified improperly or unnecessarily, or that current security considerations justify downgrading to a lower classification or upgrading to a higher classification, or that security classification guidance is improper or inadequate - is encouraged and expected to challenge the classification status. Government employees should pursue through such actions to establish agency procedures that protect individuals from retribution for bringing such actions, and to provide an opportunity for review by an impartial official or panel. And it also provide the right to appeal to the Interagency Security Classification Appeals Panel.

6. MARKING CLASSIFIED INFORMATION

Physically marking classified information with appropriate classification and control markings serves to warn and inform holders of the degree of protection required. Other notations aid in refering the derivative of the classification actions and it also facilitates the downgrading or declassification. On the other hand the marking of the classified information and material should be clearly convey the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information or material.

Below I summarize of the most commonly used document control markings. More detailed information is available via the Internet from a variety of sources.

6.1. Overall Classification Markings

The overall (i.e. highest) classification of a document is marked at the top and bottom of the outside cover (if there is one), the title page (if there is one), the first page, and on the outside of the back cover (if there is one) or on the back side of the last page.

Each interior page, which contains classified information, is marked on the top and bottom with „the overall (i.e., highest) classification of the page” sign. Each unclassified interior page is marked 'Unclassified" sign at the top and bottom. Interior pages which have „For Official

Use Only" sign, are have to be marked only at the bottom. Blank pages do not require any markings.

Attachments and annexes may be separated from the basic document. In this case they should be marked as if they were separate documents.

Additionally, every classified document must show two relevant information on the face of the document, the one of them is the name of the agency or office who classified the documantion, and the other is the date of creation process. This information must be clear enough to allow someone to receive the document, or to contact the preparing office if questions or problems arise about classification process. The computer files must be marked by appropriate headers and footers to ensure the applicable classification and associated markings are appeared in the transmitted or printed version as well. All removable storage media and devices such as diskettes, CD-ROMs, cassettes, magnet tape reels, etc. must have an outer label about the appropriate markings. Each slide must be marked on the slide itself or slide cover, as well as on the image that is projected.

7. HANDLING CLASSIFIED INFORMATION

As an approved custodian or user of classified information, has an personally responsible for the protection and control of this information. The user must safeguard this information at all times to prevent loss or compromise, unauthorized disclosure, dissemination, or duplication. Unauthorized disclosure of classified material is punishable under the criminal regulations or legislation organizational policies.

The security officer or supervisor briefs the specific rules for handling classified information which is attach the special organization. Here are some standard procedures that apply to everyone.

Classified information that is not safeguarded in an approved security container shall be constantly under the control of a person having the proper security clearance and need-to-know. An end-of-day security check should ensure that all classified material is properly secured before closing for the night.

If someone find a classified material which is left unattended (for example, in a rest room, or on a desk), it should be the user's responsibility, because the user has to ensure that the material is properly sprotected. In this case someone has to stay with the classified material and notify the security office. If this is not possible, the document or other material should be taken to the security office. The supervisor, or another person is authorized to access to this type of the information, or, if necessary, they can lock the material in your own safe overnight.

The classified material shall not be taken home, so nobody is allowed to work on classified material at home.

Classified information shall not be put in the waste basket. It must be placed in a designated container to overwhelm the classified documents by an approved method of destruction such as shredding or burning.

E-mails and the Internet create many opportunities for inadvertent disclosure of classified information. Before an user send an e-mail, post to a bulletin board, publish anything on the Internet, or add to an existing Web page, they must be absolutely certain there is none of the information is classified or sensitive unclassified information. Be familiar with the organization's policy for the use of the Internet. Many organizations require prior review of ANY information which is put on the Internet.

Classified working papers such as notes and rough drafts should be dated when it is created. They are marked with the overall classification and with the annotation "Working Papers," and disposed of with other classified waste when no longer needed.

Computer diskettes, magnetic tape, CDs, carbon paper, and used typewriter ribbons may create a problem about the security checking. As visual examination does not readily reveal whether the items contain classified information. To reduce the possibility of error, some offices treat all such items as classified even though they may not necessarily contain classified information.

Foreign government material should be stored and access controlled generally in the same manner as national. Inspite of the equivalent classification, the classified materials must be separated.

The Top Secret information is subject to continuing accountability.The official's Top Secret control are designated to receive, transmit, and maintain access and accountability records for Top Secret information. When information is transmitted from one Top Secret control official to another, the receipt is recorded and a receipt is returned to the sending official. Each item of Top Secret material is numbered in series, and each copy is also numbered.

8. APPROPRIATE USE OF COMPUTER SYSTEMS

Information Assurance (hereafter: IA) in the field of communication and information systems is the confidence that such system will protect and handle the information, and it will operate as it necessary, under the control of legitimate users. Effective IA shall ensure appropriate levels of confidentiality, integrity, availability, non-repudiation and authenticity. IA shall be based on a risk management process.

The „Communication and Information System" means any system enabling the handling of information in electronic form. A communication and information system shall contain the entire assets - including the infrastructure, organisation, personnel and information resources [4] - required to operate,.

Misuse of an automated information system is sometimes illegal, often unethical, and always reflects poor judgment or lack of care in following security rules and regulations. Misuse may create security vulnerabilities or cause damage to important information. A pattern of inability or unwillingness to follow rules for the operation of computer systems raises serious concerns about an individual's reliability and trustworthiness. As we store more and more information in computers data bases, and as these data bases become more closely linked in networks, more people have broader access to more information than ever before. The computer technology has magnified many times the ability of a careless or disaffected employee to cause severe damage.

Many aspects of computer use are governed by your organization's policy rather than by government regulation. Many government agencies and defense contractors specify the security procedures and prohibited or inappropriate activities discussed below.

8.1. Security Rules

The following are basic rules for the secure use of the computers.

- Do not enter into any computer system without authorization. Unauthorized entry into a protected or compartmented computer file is a serious security violation and is probably illegal. It can be a basis for revocation of your security clearance. Whether motivated by the challenge of penetrating the system or by simple curiosity to see what is there, unauthorized entry is a deliberate disregard for rules and regulations. It can cause you to be suspected of espionage. At the bare minimum, it violates the need-to-know principle and in some cases is an invasion of privacy.

- Do not store or process classified information on any system not explicitly approved for classified processing.
- Do not attempt to circumvent or defeat security or auditing systems without prior authorization from the system administrator, other than as part of a system test or security research authorized in advance.
- Do not install any software on your computers without the approval of your system administrator.
- Do not use another individual's user ID, password, or identity.
- Do not permit an unauthorized individual (including spouse, relative or friend) access to any sensitive computers network. Do not leave sensitive but unclassified work materials on a home computers to which other persons have access.
- Do not reveal your password to *anyone* -- not even your computers system administrator.
- Do not respond to any telephone call from anyone whom you do not personally know who asks questions about your computers, how you use your computers, or about your user ID or password.
- If you are the inadvertent recipient of classified material sent via e-mails or become aware of classified material on an open bulletin board or web site, you must report this to the security office.
- Do not modify or alter the operating system or configuration of any system without first obtaining permission from the owner or administrator of that system.
- Do not use your office computers system to gain unauthorized access to any other computers systems.

8.2. Inappropriate Use

Many offices permit some minimal personal use of official equipment when such personal use involves minimal expense to the organization. This is performed on someone's personal non-work time, which does not interfere with the mission of the office, and does not violate standards of ethical conduct.

The following activities are considered to be misuse of office's equipment:

- The creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials can cause to be fired.
- Annoying or harassing another individual, for example through uninvited e-mails of a personal nature or using lewd or offensive language can cause to be fired.
- Using the computers for commercial purposes or in support of "for-profit" activities or in support of other outside employment, business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services), or gambling.
- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings.
- Any activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Use for posting office information to any external newsgroups, chat rooms, bulletin boards, or other public forums without prior approval.

- Any personal use that could cause congestion, delay, or disruption of service to any office equipment. This includes sending pictures, videos, or sound files or other large file attachments that can degrade computers network performance.
- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information. This includes copyrighted computers software; other copyrighted or trademarked materials or materials with intellectual property rights (beyond fair-use); privacy information; and proprietary data or export-controlled data or software.

9. E-MAIL

There are two big problems with e-mails; one of them is the increased risk of accidental security compromise; the other is sending inappropriate materials by e-mail, which has caused many people to be fired.

9.1. Security Risks with E-Mail

As a result of the Internet and e-mail, there has been a sharp increase in security incidents involving the accidental disclosure of classified and other sensitive information. One common problem occurs always when individuals download a seemingly unclassified file from a classified system, and then fail to carefully review this file before sending it as an attachment to an e-mail message. Too often, the seemingly unclassified file actually has some classified material or classification markings that are not readily apparent when the file is viewed on line. Sending such material by e-mail is a security violation even if the recipient has an appropriate security clearance, as e-mail can easily be monitored by unauthorized persons.

More important, even if the downloaded file is really unclassified, the electronic version of that file may have recoverable traces of classified information. This happens because data is stored in "blocks." If a file does not take up an entire block, the remainder of that block may have recoverable traces of data from other files. The administrator system must follow an approved technical procedure for removing these traces before the file is treated as unclassified.

Some organizations have found to lock their computers drives to prevent any downloading of files from the classified system. If necessary to download and retransmit an unclassified file from a classified system, the file must be downloaded and processed by the system administrator to remove electronic traces of other files before it is retransmitted.

9.2. Inappropriate Materials

Sending e-mail is like sending a postcard through the mail. Just as the mailman and others have an opportunity to read a postcard, network eavesdroppers can read your e-mail as it passes through the Internet from computer to computer. E-mail is not like the secrecy of correspondence, where your privacy rights are protected by law.

The courts have repeatedly sided with employers who monitor their employees' e-mail or Internet use. A 2005 survey found that 63% of corporations with 1,000 or more employees either employ or plan to employ staff to read or otherwise analyze outbound email. 27% of the companies reported terminating an employee due to email misuse during the previous year. 35% investigated a suspected email leak of confidential information during the past year. In addition to protection of their intellectual property, companies were concerned about compliance with financial disclosure regulations.

Organizations also monitor email to protect themselves against lawsuits, as the organization can be held liable for abusive, harassing, or otherwise inappropriate messages sent over its computers network.[2]

10. SECURITY OF HARD DRIVES

Secrets in the computers require the same protection as secrets on paper. This is because information can be recovered from a computers hard drive even after the file has been deleted or erased by the computers user. It is estimated that about a third of the average hard drives contains information that has been "deleted" but it is still recoverable.

When someone deletes a file, most computers operating systems delete only the "pointer", which allows the computer to find the file on the hard drive. The file itself is not deleted until it is overwritten by another file. This is comparable to deleting a chapter heading from the table of contents of a book, but not removing the pages on which the chapter is written. Some networks may be configured to "wipe" or purge the hard drive when information is deleted, but most are not.

Computers on which classified information is prepared must be kept in facilities that meet specified physical security requirements for processing classified information. If necessary to prepare classified information on a computer in a non-secure environment, erybody has to use a removable hard drive or laptop that is secured in an approved safe when it is not in use. Alternatively, they can use a typewriter.

11. COMPUTER PASSWORDS

Passwords are used to authenticate an individual's right to have access to certain information. A password could be use only personally. Lending it to someone else is a security violation and may result in disciplinary action against both parties. Never disclose your password to anyone. Memorize it – do not put it in writing. If someone leave the terminal unattended for any reason, log off or use a screen lock. Otherwise, someone else could use the computer to access information, they are not authorized to have. Someone will be held responsible if anybody else uses other password in connection with a system transaction.

As hackers and scammers develop more clever ways to steal passwords, it becomes more important that passwords be changed regularly. Use a password with at least six and preferably eight characters and consisting of a mix of upper and lower case letters, numbers, and special characters such as punctuation marks. This mix of various types of characters makes it more difficult for a hacker to use an automated tool called a "password cracker" to discover your password. Cracking passwords is a common means by which hackers gain unauthorized access to protected systems.

12. "SOCIAL ENGINEERING"

"Social engineering" is hacker-speak for conning legitimate computers users into providing useful information that helps the hacker gain unauthorized access to their computers systems.

---

[2] In the past couple of years, The New York Times fired 23 employees for exchanging off-color e-mails. Xerox fired 40 people for inappropriate Internet use. Dow Chemical fired 24 employees and disciplined another 230 for sending or storing pornographic or violent material by e-mail. Several years ago, Chevron Corp. had to pay $2.2 million to plaintiffs who successfully brought a suit of sexual harassment, in part because an employee sent an e-mail to coworkers listing the reasons why beer is better than women.

The hacker using social engineering usually poses as a legitimate person in the organization (maintenance technician, security officer, inexperienced computer user, VIP, etc.) and employs a plausible cover story to trick computer users into giving useful information. This is usually done by telephone, but it also may be done by forged e-mail messages or even in-person visits.

Most people have an incorrect impression of computers break-ins. They think they are purely technical, the results of technical flaws in computers systems which the intruders are able to exploit. However, the truth is that social engineering often plays a big part in helping an attacker slip through security barriers. Lack of security awareness or gullibility of computer users often provides an easy stepping stone into the protected system if the attacker has no authorized access to the system at all.

13. PROTECTING YOUR HOME COMPUTER

If someone access own office network from home or do work at home that is emailed to the office or brought to the office on any removable storage media. This can affect the security of the office network. If someone has an obligation to take standard procedures for protecting own home computer against viruses and other problems, it might be transmitted to own office network. These include installing a virus checker with automatic updates, installing a personal firewall, turning off or uninstalling any options that significantly increase security risk, and keeping the operating system of own computer up-to-date with security fixes as they become available.

14. SECURITY VIOLATIONS

A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results. No matter how minor, any security infractions must be reported immediately to the security office so that the incident may be evaluated and any appropriate actions taken.

14.1. Deliberate Violation[3]

[6] Any deliberate violation of security rules or regulations is a significant concern, as it may indicate indifference toward national security or a general inability or unwillingness to abide by the security regulations.

Any deliberate revelation of classified or other protected information to any unauthorized person is a particularly egregious offense. Examples of this include:

- Leaking protected information to journalists or others in an effort to influence Government policy.
- Giving protected information to a private company or corporation to pursue some personal business interest or to pave the way for seeking a job there, or to help a relative or friend in their business even if not done for personal gain.
- Giving protected information to a friend or business associate just to impress them with one's importance.

[3] Naval Intelligence analyst Jonathan Jay Pollard passed several classified political and economic analyses to three different friends whom he felt could use the information in their business. Although Pollard hoped to get some benefit in return, his principal motive was simply to impress his friends with his knowledge and the importance of his work. Willingness to sacrifice security for minor personal gain indicates a degree of narcissism that is a serious concern. This attitude can be dangerous and may portend future problems. In Pollard's case, for example, his need to feel important and to have others validate that importance subsequently led him to volunteer his services to Israeli Intelligence. He is now serving a life term in prison.

14.2. Pattern of Negligence or Carelessness

[6] A pattern of routine security violations due to negligence, carelessness, inattention, or a cynical attitude toward security discipline is potentially disqualifying regardless of whether or not information was actually compromised.

14.3. Major Violations[4]

The significance of a security violation does not depend upon whether information was actually compromised. It depends on the intentions and attitudes of the individual who committed the violation.

Ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining your security clearance. Although accidental and infrequent minor violations are expected to deliberate or repeated failure to follow the rules is definitely not. It may be a symptom of underlying attitudes, emotional, or personality problems that are a serious security concern.

The following behaviors are of particular concern and may affect your security clearance:

- A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline.
- Taking classified information home, ostensibly to work on it at home, or carrying it while in a travel status without proper authorization.
- Prying into projects or activities for which the person does not have (or no longer has) a need to know. This includes requests for classified publications from reference libraries without a valid need to know, or any attempt to gain unauthorized access to computers systems, information, or data bases.
- Intoxication while carrying classified materials or that causes one to speak inappropriately about classified matters or to unauthorized persons.
- Deliberate revelation of classified information to unauthorized persons to impress them with one's self-importance.
- Copying classified information in a manner designed to obscure classification markings. This may indicate intent to misuse classified information.
- Making unauthorized or excessive copies of classified material. Going to another office to copy classified material when copier equipment is available in one’s own work area is a potential indicator of unauthorized copies being made.
- Failing to report requests for classified information from unauthorized individuals.
- Leaving a classified file or security container unlocked and unattended either during or after normal working hours.
- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.
- Reproducing or transmitting classified material without proper authorization.
- Losing one’s security badge.
- Removing classified material from the work area in order to work on it at home.
- Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know.

[4] Storing classified information at home is **a** very serious concern as it may indicate current or potential future espionage. At the time of their arrest, many well-known spies were found to have large quantities of classified documents at their residences. [5] CIA spy Aldrich Ames had 144 classified documents at his home, while Edward Moore had 10 boxes of CIA documents at home. Of various Navy spies, Jonathan Pollard had a suitcase full of classified materials, Michael Walker had 15 pounds of classified material, while Samuel Morison had two portions of Navy documents marked Secret.

- Discussing classified information over the telephone, other than a phone approved for classified discussion.
- Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard.
- Carrying safe combinations or computers passwords (identifiable as such) on you, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computers.
- Failure to mark classified documents properly.
- Failure to follow appropriate procedures for destruction of classified material.

Failure to report a security violation is itself a security violation and may be a very serious concern!

15. CONCLUSION

Based on international experience which can demonstrate, that the protection of classified information has a lot of components. In this article I have highlighted some of these important areas. I find personal safety very important because it creates the foundation for the protection of classified information. I have written down the rating regulations from the field of administrative security because this is important. A need to know is a very important element of security. The ratings data management policy is explained to me, because it is an essential prerequisite for daily work. In the case of a breach of security, it is very important to minimize the damage, therefore the basic rules are described. Rated datas are produced and handled on modern computing devices in the 21st century._ The most important rules of electronic handling are described as well. As described, the above demonstrate that the most efficient way you can ensure classified information is to use safety areas in a coordinated way.

References:

[1] A minősített adat védelméről szóló 2009. évi CLV. törvény

[2] A nemzeti biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről szóló 90/2010.(III.26.) Korm. rendelet

[3] A minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól szóló 161/2010.(V.6.) Korm. rendelet

[4] COUNCIL DECISION of 31 March 2011 on the security rules for protecting EU classified information (2011/292/EU)

[5] SECURITY WITHIN THENORTH ATLANTIC TREATY ORGANISATION Corrigendum to C-M(2002)49 dated 17 June 2002Amendment 3

[6] http://www.dhra.mil/perserec/adr/handlinginfo/handlingtext.htm; (2012. 01. 06.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Munk Sándor
munk.sandor@uni-nke.hu

AZ INFORMATIKAI IRÁNYÍTÁS RENDJE, FELADATAI

Absztrakt

A korszerű informatika szolgáltatásai, a szolgáltatások feltételeinek megteremtésére, nyújtására és igénybevételére irányuló informatikai tevékenységek tervezettsége, szervezettsége, egységes irányítása alapvetően határozza meg a szervezetek, szakterületek, társadalmi tevékenységi szférák működésének eredményességét, minőségét. A szakirodalom eddig kevéssé foglalkozott az informatikai irányítás kérdéseivel olyan összetett szervezetrendszerekben, mint a közigazgatás és a védelmi szféra szervezetei. Az informatikai irányítás feladatainak elemzése előfeltétele egy informatikai irányítási rendszer kialakításának, a jog- és feladatkörök meghatározásának, illetve egy ilyen rendszer értékelésének. Jelen publikáció bemutatja az informatikai irányítás feladatainak egy lehetséges csoportosítását és meghatározza az egyes feladatok alapjait, főbb jellemzőit.

Planning, organization, and direction of activities producing and utilizing IT services fundamentally determines the operational effectiveness and quality of organizations, professional areas, social activity spheres. The professional literature so far hardly addressed the issues of IT management in such complex organizational structures, as public administration, and defense sphere organizations. Analysis of IT management tasks is necessary for implementing an IT management system, determining the rights and responsibilities, and assessing such a system. Recent publication presents a classification of IT management/control tasks, and determines their basics, main characteristics.

***Kulcsszavak**: informatikai vezetés és irányítás, az informatikai irányítás feladatai, jog- és feladatkörök ~ IT management, IT management tasks, rights and responsibilities*

1. BEVEZETÉS

A korszerű informatika szolgáltatásai, a szolgáltatások feltételeinek megteremtésére, nyújtására és igénybevételére irányuló informatikai tevékenységek tervezettsége, szervezettsége, egységes irányítása ma már alapvetően határozza meg a szervezetek, szakterületek, társadalmi tevékenységi szférák működésének eredményességét, minőségét. Mint azt egy korábbi, az informatikai irányítás alapjait feldolgozó publikációban [1] már megfogalmaztuk, az olyan összetett szervezetrendszerekben, mint a közigazgatás rendszere, a védelmi szféra intézményei (Magyar Honvédség, Magyar Rendőrség, a katasztrófavédelem rendszere) az informatikai irányítás, mint a vezetés és működés feltételeit biztosító tényező, lényeges, sőt egyre növekvő jelentőségű szerepet játszik. Ennek ellenére az informatikai irányítás fogalmával, tartalmával foglalkozó tudományos és szakmai publikációk köre rendkívül szűkös, közigazgatási, védelmi szférabeli, honvédségi szintű vizsgálatuk lényegében hiányzik.

A hivatkozott publikációban foglaltakra alapozva informatikai (szakmai) irányítás alatt az informatikai szakmai ügyekre, tevékenységekre vonatkozó irányítási jogkörök és feladatok összességét értjük, amelynek rendeltetése az irányított szervezetek informatikai tevékenységeinek az alaprendeltetést, a szervezeti célkitűzéseket támogató, eredményes és hatékony megvalósításának biztosítása. Informatikai tevékenységek közé tartoznak mindazon tevékenységek, amelyek az informatikai eszközök, rendszerek szolgáltatásainak a szervezeti célkitűzéseket szolgáló, hatékony igénybevételére, valamint az informatikai szolgáltatások feltételeinek kialakítására (továbbfejlesztésére) és fenntartására irányulnak.

Az informatikai irányítás rendjének, feladatainak vizsgálata, a kapcsolódó fogalmak értelmezésének tisztázása megítélésünk szerint alapfeltétele egy összetett szervezetrendszeren belüli informatikai irányítás célirányos kialakításának és hatékony megvalósításának, az ehhez szükséges jog- és feladatkörök meghatározásának, illetve egy informatikai irányítási rendszer ellenőrzésének és értékelésének.

A fentiek alapján jelen publikáció alapvető célja, hogy elemezze és összegezze az informatikai irányítás rendjét és feladatait. Ezen belül:

- bemutassa az informatikai irányítás feladatainak egy lehetséges csoportosítását;
- és meghatározza az egyes feladatok tartalmát, főbb jellemzőit.

2. AZ INFORMATIKAI IRÁNYÍTÁS RENDJE, FELADATAI

A vezetés funkcióival, feladataival kapcsolatban a szakirodalomban nincs egységesen elfogadott álláspont, Henri Fayoltól és Frederick Winston Taylortól kezdődően számos felosztással, csoportosítással találkozhatunk. Ezek többnyire nem egymásnak ellentmondó, hanem eltérő nézőpontokat, vagy eltérő hangsúlyokat megjelenítő felsorolások, értelmezések. Ennek megfelelően nem található széles körben elfogadott értelmezés az informatikai vezetés, vagy irányítás feladatrendszerére vonatkozóan sem. Az idők során különböző informatikai vezetési iskolák, megközelítések[1] jelentek meg, amelyek mindegyike megfogalmazta az informatikai vezetés és irányítás feladataira vonatkozó saját elképzeléseit.

Jelen publikáció nem tűzte ki céljául az informatikai vezetés és irányítás feladatai különböző megközelítéseinek összehasonlító elemzését és ennek alapján egy új "tökéletes" feladatrendszer meghatározását. Ehelyett közigazgatási és védelmi szférabeli informatikai irányító szervek szervezeti és működési szabályzatokban szereplő feladatrendszerét [2; 3; 4] kiindulópontként felhasználva mutat be egy csoportosítást, amely további vizsgálatok tárgyát

[1]Informatikai rendszer-menedzsment, információs erőforrás-menedzsment, informatikai szolgáltatás-menedzsment, informatikai stratégiai menedzsment, informatikai menedzsment.

képezheti. Ennek megfelelően a – hatékony és eredményes szakmai irányítás érdekében – az informatikai irányítás, az informatikai irányító szerv feladatai közé tartozik (tartozhat):

- informatikai jövőképek, szakpolitikák, stratégiák, stratégiai tervek kidolgozása, részvétel a szervezeti szintű stratégia kialakításában, közreműködés más szakterületek stratégiai dokumentumainak kidolgozásában;
- informatikai szabályozók kidolgozása, közreműködés más szervezeti szabályozók kidolgozásában;
- döntés, jóváhagyás, egyetértés, véleményezés informatikai szakmai ügyekben;
- az informatikai tevékenységek tervezése, szervezése, koordinációja;
- alárendelt szervezetek közvetlen és szakmai irányítása;
- az informatikai tevékenységek felügyelete, ellenőrzése;
- az informatikai szakterület képviselete.

A fentiek nélkül egy szervezeten belül az informatikai szakterület irányítása nem lehetséges, így a továbbiakban sorra vesszük ezen feladatok tartalmát, jellemzőit.

3. STRATÉGIAI TERVEZÉSI FELADATOK

Az informatikai tevékenységek szervezeti célokat, folyamatokat támogató tervszerű, hatékony megvalósításának, eredményes irányításának feltétele a szervezet hosszú távú célkitűzései megvalósítását támogató stratégiai informatikai dokumentumok, tervek megléte.

Az informatikai stratégiai dokumentumok egy *stratégiai dokumentum-rendszer* részét képezik, amelynek alapját a szervezeti szintű, átfogó stratégiai dokumentumok alkotják. Az informatikai – és más szakterületi – hosszú távú elképzeléseknek, terveknek a szervezeti stratégiai elképzeléseket, terveket kell támogatniuk, szolgálniuk és egymással is összhangban kell állniuk.

Az informatikai vezetés, irányítás egyik alapvető feladata a hosszú távú informatikai dokumentumok kidolgozásának, felülvizsgálatának biztosítása. Ezek közül az informatikai stratégia szükségessége széles körben elfogadott[2], az ezt megalapozó (jövőképek, szakpolitikák[3]), vagy részletező dokumentumok (tervek) kidolgozása azonban általában szervezetfüggő.

Az *informatikai stratégiai dokumentumok* kidolgozása, illetve a kidolgozás irányítása, koordinálása a felső szintű informatikai irányító szerv feladata, felelőse a szervezet informatikai vezetője. A kidolgozásba a szükséges mértékben be kell vonni az alacsonyabb szintű informatikai irányító szerveket, illetve informatikai szervezeteket. A dokumentumok jóváhagyója a szervezet felső vezetése (vezetője). Az informatikai stratégiai tervezés támogatására módszertanok állnak rendelkezésre.

A felső szintű informatikai irányításnak nem csak a szervezeti jövőkép, stratégia informatikai szakterületre történő lebontása a feladata, hanem az aktív *részvétel a szervezeti jövőkép, stratégia kialakításában*. Ennek során a szakterületet irányító informatikai vezetőnek szervezeti megközelítésben kell megjelenítenie, érvényesítenie az informatika szervezeti célokat szolgáló lehetőségeit, szolgáltatásait. Ezen belül egyrészt közvetítenie kell, hogy az informatika a felmerülő jövőképeket, stratégiai célokat, elképzeléseket milyen mértékben, milyen várható eredménnyel képes támogatni, másrészt önálló javaslatokat is tehet a jövőkép egyes informatikai jellegű elemeire, az informatika révén kitűzhető szervezeti célokra, megoldásokra, illetve az ezeket megvalósító informatikai fejlesztési irányokra, feladatokra.

[2] A Magyar Köztársaságban például a kormány irányítása alatt álló központi közigazgatási szervek és irányításuk, valamint felügyeletük alá tartozó közigazgatási szervek informatikai stratégia készítésére kötelezettek.

[3] Vision [statement], policy.

Végül a felső szintű informatikai irányítás feladata a *közreműködés más funkcionális, szakterületi stratégiák kidolgozásában, véleményezésében*. A szervezet stratégiai dokumentum-rendszerének további összetevői[4] is szorosan kapcsolódnak az informatikai stratégiai elképzelésekhez, tervekhez: célokat, feladatokat határoznak meg; megvalósulásuk informatikai támogatást feltételez; informatikai elképzelések, tervek megvalósulását támogatják, befolyásolják. Ebből következően az informatikai szakterület véleményének, javaslatainak felhasználása a stratégiai dokumentumok összehangoltságának alapvető feltétele.

4. SZABÁLYOZÁSI FELADATOK

A magatartási, cselekvési *szabályok* a szervezeti tevékenység, az eredményes és hatékony működés legfontosabb kereteit, alapvető feltételét képezik. A társadalmi szabályok (normák) olyan magatartási előírások, amelyek meghatározott feltételek fennállása esetén a lehetséges magatartások közül kijelölik a helyeset, a követendőt. A szabályok lehetnek jogszabályok, szakmai szabályok, vagy erkölcsi (íratlan) szabályok.

A *szabályozás*, mint tevékenység, valamely tevékenységi körre vonatkozó szabályok – feladatok, felelősségi és hatáskörök, előírások és korlátozások – meghatározására irányuló tevékenység. A szabályozás elsősorban a rendszeresen ismétlődő tevékenységek végrehajtásának szakmai, technikai, vagy eljárási szabályait rögzíti. Hatókörét és tárgyát tekintve többek között lehet nemzetközi, nemzeti, vagy szervezeti, illetve átfogó és szakterületi, ezen belül részterületi. A szabályozás eredményei alapvetően írásban, különböző típusú szabályozó dokumentumokban jelennek meg.

Az *informatikai szabályozás* egy szakterületi szabályozás, amelynek rendeltetése az informatikai tevékenységek – az informatikai szolgáltatások igénybevételére, valamint a szolgáltatások feltételeinek kialakítására (továbbfejlesztésére) és fenntartására irányuló tevékenységek – szabályozása.

Az informatikai szabályozás és az így kialakított szabályozók rendszere szintekre tagolható. Szervezeti szempontból három szabályozási szintet különböztethetünk meg. Az első szintet a külső, szervezeten kívüli, a szervezetre is vonatkozó (nemzetközi, szövetségi, nemzeti) szabályozás képezi. A második szint a szervezet egészére vonatkozó, alapvető szabályokat rögzítő átfogó szervezeti szabályozás szintje. Végül a harmadik szinthez az átfogó szervezeti szabályozóknak alárendelt, alacsonyabb szintű szabályozók tartoznak.

A szervezeti szintű informatikai szabályozás eredményei megjelenhetnek:

- nem informatikai szabályozókban (szervezeti és működési szabályzat, munkaköri leírás, nem informatikai szakterületi szabályozók);
- átfogó informatikai szabályozóban (szabályzatban);
- szabályozási területenként kiadott önálló informatikai szabályozókban;
- valamint informatikai rendszer (hálózat-) szintű szabályozókban.

Az *informatikai szabályozás feladatai* közé mindenekelőtt az informatikai szabályozó rendszer kialakítása, valamint az egyes informatikai szabályozó dokumentumok kidolgozása, illetve felülvizsgálata tartozik. Az informatikai szabályozó rendszer kereteit külső és szervezeti szabályozók, illetve a szervezeti szabályozó rendszer felépítése határozzák meg. Az informatikai szabályozó rendszer, illetve egyes részeinek kialakítása az illetékes informatikai irányító szervek feladata.

Az informatikai szabályozók előkészítése, kidolgozása az informatikai irányító szervek felelőssége, a konkrét kidolgozás a tartalomtól, terjedelemtől függően lehet az irányító szerv feladata, a kidolgozásba bevonhat szakértőket, vagy arra létrehozhat kidolgozó

[4] Humánpolitikai, logisztikai, pénzügyi, marketing, fejlesztési, biztonsági, ügyfélkapcsolati, stb. stratégia.

munkacsoportot. A kidolgozott szabályozó dokumentumok tervezetét a kibocsátás előtt az előírt szervekkel, testületekkel egyeztetni, véleményeztetni kell, az érintettekkel pedig véleményeztetni célszerű.

Az informatikai irányítás feladatkörébe tartozik a *más szabályozók kidolgozásában történő részvétel* is, ami magában foglalja az átfogó szervezeti szintű szabályozókba, vagy más szakterületek (pld. logisztikai, pénzügyi, beszerzési, stb.) szabályozóiba történő bedolgozást, illetve a szabályozók véleményezését.

5. TERVEZÉSI FELADATOK

A *tervezés* lényegét tekintve előrelátás, a jövőbeni cselekvések irányainak és feltételeinek meghatározása, rendszerbe foglalása, olyan céltudatos tevékenység, amely a múlt és a jelen információira, elemzésére építve, valamint a jövőben várható körülményeket figyelembe véve meghatározza a célok, jövőbeni feladatok megvalósítását biztosító cselekvési programot. A tervezés, mint vezetési funkció, tehát a kitűzött célok elérését biztosító cselekvési változat[ok] (végrehajtandó feladatok) meghatározása.

A *terv* a tervezés eredménye, amely általában tartalmazza a jövőbeni működésre vonatkozó célokat, valamint az ehhez szükséges tevékenységeket és erőforrásokat, vagyis azt, hogy kinek, mit, mikor, milyen sorrendben és milyen eszközök, erőforrások felhasználásával kell megtennie.

A tervek időtávjuk szerint lehetnek stratégiai (hosszú távú), taktikai (középtávú), illetve operatív, (rövidtávú) tervek[5] és csoportosíthatóak a végrehajtásban érintettek köre, valamint a felölelt tevékenységrendszer (szakterület, vagy funkcionális terület) alapján: ki[k]nek a terve, milyen feladatokra és milyen időtávra. Egy szervezeten belül a különböző terveknek időtáv és szakterületek szerint is egymásra épülő, összehangolt rendszert kell alkotniuk.

Az *informatikai tervezés* olyan szakterületi tervezés, a kitűzött célok elérését biztosító informatikai feladatok, tevékenységek körének és végrehajtási rendjének meghatározása. Az informatikai tervezés eredményei megjelenhetnek más szervezeti, vagy szakterületi tervek részeiként, vagy önálló informatikai tervek formájában.

Az informatikai tervek közé tartoznak többek között:

- az informatikai szervezetek, szervezeti egységek éves és havi munkatervei;
- a rendszeresen kidolgozandó részterületi, vagy funkcionális tervek;
- valamint az egyedi feladatokhoz (műveletekhez, projektekhez) kapcsolódó [feladat]tervek.

Az *informatikai tervezés feladatai* az irányító és a végrehajtó szervek, szervezetek esetében eltérő módon jelennek meg. Az informatikai irányító szervek esetében kiemelt szerepet a fejlesztési és beszerzési tervek, valamint az egyedi feladatokhoz kapcsolódó tervek játszanak. A végrehajtó szervek, szervezetek munkaterveket, illetve részterületi, vagy funkcionális (üzemeltetési, továbbképzési, stb.) terveket készítenek.

A jellemzően program/projekt-alapú informatikai fejlesztési és beszerzési tervek kidolgozása az informatikai irányító szervek feladata, amelynek alapját az informatikai stratégiában, illetve a hosszabb időtávú tervekben foglaltak képezik. A fejlesztési, beszerzési tervek az irányított szervezetek javaslatai figyelembevételével, a szervezet tervezési rendszerébe illeszkedő módon, más szakterületi tervekkel összehangoltan kerülnek kidolgozásra, majd az irányított szervezetek számára visszabontásra. Az informatikai fejlesztési, beszerzési feladatok megjelenhetnek önálló informatikai fejlesztési programok, projektek formájában, vagy más fejlesztési programok, projektek részeként.

[5] Különböző körülmények között az időtávok lehetnek: 5-10 év, 3-5 év és 1-3 év, illetve 3-5 év, 1-3 év és 1 év, vagy kevesebb.

Az egyedi feladatokhoz (műveletekhez, projektekhez) kapcsolódó informatikai feladattervek kidolgozása az adott feladatért felelős vezető szerv informatikai irányító szervének feladata, ami lehet önálló terv, vagy egy átfogó feladatterv része.

6. DÖNTÉS, JÓVÁHAGYÁS, EGYETÉRTÉS, VÉLEMÉNYEZÉS

A döntés, jóváhagyás, egyetértés, véleményezés szakmai ügyekben az irányítási jogviszony egyik alapvető összetevője, az irányító szerv jogköre, lehetősége az irányított szervek döntési jogainak átvételére, vagy megosztására. [6] Az irányító szerv konkrét ügyekben hozott döntései jellemzően szervi ügyeket érintenek, mivel a szakmai ügyekben történő döntés az irányított szerv alaprendeltetését érintő hatáskör elvonását jelentené.

Az irányító és az irányított közötti *döntési hatáskörmegosztás típusai* négy csoportba sorolhatóak:

- az irányított döntéstervezetének irányítói véleményezése;
- az irányított szerv döntéséhez való előzetes irányítói hozzájárulás;
- az irányított döntésének utólagos jóváhagyása;
- javaslattétel az irányítói döntéshez az irányított részéről.

Az első három az irányított szerv, az utolsó pedig az irányító szerv döntéséhez, azok előkészítéséhez és meghozatalához kapcsolódik és az irányított szerv egyre csökkenő döntési hatáskörét eredményezi.

Az informatikai irányítás esetében *a döntési hatáskörmegosztás jellemző területei* közé szervi és szakmai kérdések egyaránt tartoz(hat)nak. Ilyenek többek között a következőek:

- informatikai tevékenységet ellátó szervezetek, szakmai beosztások létrehozása (megszüntetése), átalakítása, módosítása, illetve személyügyi döntések meghozatala;
- informatikai tevékenységet ellátó szervezetek általános feladatainak, működési rendjének meghatározása, módosítása (külső és belső szabályozók, Szervezeti és Működési Szabályzat);
- informatikai, illetve kapcsolódó jövőképek, szakpolitikák, stratégiai dokumentumok;
- informatikai, illetve kapcsolódó (pld. fejlesztési, beszerzési) tervek, intézkedések;
- informatikai, illetve kapcsolódó fejlesztési döntések, dokumentumok, beszerzési szerződések;
- az informatikai szakterületet érintő más előterjesztések, javaslatok.

Az informatikai irányító szervek – az alkalmazásért viselt felelősséghez kapcsolódóan – mellérendelt jogviszonyban célszerűen az informatikai ellátás és technikai kiszolgálás területén is rendelkeznek véleményezési, vagy egyetértési jogkörrel.

7. SZERVEZÉS, KOORDINÁCIÓ

A *szervezés*, mint a vezetési folyamat része, lényegét tekintve az erőforrások meghatározása, elosztása, összerendezése, a végrehajtáshoz legcélszerűbb működési struktúra kialakítása a döntés során kiválasztott cselekvési változat megvalósítása érdekében. A szervezés során történik meg az átfogó cél, feladat lebontása az alárendelt, irányított szervezetek, szervek, személyek elé kitűzött részcélokra, részfeladatokra és szükség esetén ezekhez erőforrások rendelése. A szervezés kiterjedhet a szervezeti struktúrára, a szervezeti folyamatokra és a konkrét feladatvégrehajtásra.

[6] Az egyetértési és véleményezési jog nem csak irányító és irányított, hanem mellérendelt szereplők esetében is értelmezhető.

A *koordináció* a szervezéshez szorosan kapcsolódó vezetési, irányítási funkció, amelynek lényege az eltérő feladatokkal és hatáskörökkel rendelkező, de egymással szoros kapcsolatban álló szervezetek, szervek, személyek működésének, tevékenységének (meghatározott feladatok végrehajtásának) előzetes és menet közbeni összehangolása. Tervezéssel és szervezéssel nem lehet minden összhang hiányt kezelni, illetve számos olyan összehangolást igénylő probléma merülhet fel, amelyek nem teszik szükségessé a kitűzött célok módosítását, a tervek megváltoztatását, illetve a szervezeti-, vagy folyamatstruktúrába történő tartós beavatkozást.

A koordináció a szervezeten belüli munkamegosztás következménye és velejárója. Ha a folyamatokat időben, térben, mennyiségben részeire bontják és a részfeladatokat más-más, az adott feladatra specializálódott szervezeti tagok, csoportok végzik el, akkor alapvető vezetői feladat ezek tevékenységének összehangolása, szervezése. Koordinációt igényelhetnek a menetközben felmerülő, a tervek által részleteiben nem szabályozott kérdések, problémák is.

Koordinációra szükség lehet, és az megvalósulhat a szervezeti hierarchiához igazodóan, amikor is a magasabb szinten lévő vezető az alárendeltek (az irányított szervezetek, szervek, személyek) tevékenységét hangolja össze, azonban a szervezetek működésében jelentősebb szerepet játszik az alapvető szervezeti (közigazgatásban ágazati) struktúrákon átlépő, úgynevezett horizontális szakterületek, szakfeladatok koordinációja.

A szakterületi, *szakmai koordináció* a szakmai irányítás egyik alapvető összetevője, a szakterületért felelős vezető egyik feladata, amellyel hozzájárul, hogy a szakterületi tevékenységek eredményesen és hatékonyan szolgálják a szervezeti célkitűzések megvalósítását. A szakmai koordináció megvalósításának feltétele az illetékes vezető megfelelő jogköre. A NATO a koordinációs jogkör tartalmát az érintettek közötti konzultáció igénylésében, a megállapodás tárgyalásos úton történő kialakításában és ennek hiányában a kérdés illetékes hatóság elé utalásában határozza meg (a jogkör nem foglalja magában a megállapodás kikényszerítését). [5, 2-C-16 o.]

Az *informatikai koordináció* tehát egymással egyenrangú (mellérendelt) szervezetek, szervek, személyek informatikai szaktevékenységeinek összehangolása. A koordináció szerepe, jelentősége annál nagyobb, minél szorosabb az informatikai szaktevékenységek közötti kapcsolat, minél erősebb a szakmai együttműködés. Eszköze közé tartozhat a rendszeres, vagy eseti koordinációs megbeszélés, értekezlet, összetettebb feladatok esetében pedig az érintett szervezetek képviselőiből létrehozott munkacsoport is.

8. SZAKTERÜLETI KÖZVETLEN ÉS SZAKMAI IRÁNYÍTÁS

A szakmai irányító szervek alapvető feladata az irányítás tárgyát képező szervezetekben folyó szakmai tevékenység irányítása (meghatározott cél elérését biztosító befolyásolása). Az irányítási jogkörök tekintetében az érintett szervezetek két nagy csoportba sorolhatóak. Az elsőbe azon – alapvetően szakmai – szervezetek tartoznak, amelyek az irányító szerv közvetlen, hierarchikus alárendeltségében állnak. A nagyobb csoportot azon szervezetek alkotják, amelyek felett az irányító szervnek 'csak' szakmai, hierarchián kívüli irányítási jogkörei vannak. Az ezekre vonatkozó szakmai irányítás kérdéseit részletesebben már korábban tárgyaltuk.

Az informatikai irányító szervek által gyakorolt *közvetlen informatikai irányítás* alá különböző alaprendeltetésű informatikai szervezetek tartozhatnak. Az informatikai szaktevékenységek csoportosításának megfelelően ezek elsősorban fejlesztéssel, üzemeltetéssel, anyagi-technikai kiszolgálással, ellátással foglalkozó, vagy ezen funkciókat integráló szervezetek lehetnek, de létrehozhatóak speciális támogató (oktatási-képzési, tudományos kutatási, tájékoztató, stb.) tevékenységeket végző szervezetek is. A közvetlen irányítás jogköre az elérendő célok és a végrehajtandó feladatok meghatározása mellett

tartalmazhatja a kívánt tevékenységek előírását is, amelyek egyedi döntésekkel, operatív beavatkozásokkal biztosíthatóak.

Napjainkban a szervezeti önállóság és felelősség növelése érdekében informatikai területen is egyre inkább a közvetlen irányítás korlátozottabb formái kerülnek előtérbe, a szakmai irányítástól pedig elmozdulás tapasztalható a szakmai felügyelet irányába.

9. FELÜGYELET, ELLENŐRZÉS

Az informatikai tevékenységek felügyelete, ellenőrzése minden szinten az informatikai (szakmai) irányítás egyik alapvető eszköze, amelynek lényege – a korábban elmondottaknak megfelelően – az érintett szervezetek működésének figyelemmel kísérése és az előírtaktól eltérő működés, tevékenység esetén, megfelelő jogkörök birtokában beavatkozás.

Az ellenőrzés általánosságban lehet belső, külső és társadalmi, ezen belül a belső ellenőrzés témánk szempontjából lényeges típusa a folyamatokba épített előzetes és utólagos vezetői ellenőrzés (FEUVE). A felügyelet alapvető típusai: a teljes tevékenységre kiterjedő (de az irányításnál szűkebb jogkörű) általános felügyelet; meghatározott, szabályozókban körülhatárolt tevékenységre vonatkozó speciális (szakmai, szak-) felügyelet; valamint a működés jogszerűségére irányuló törvényességi felügyelet.

Az *informatikai (szak)ellenőrzés* a hierarchikus irányítás (felügyelet), vagy szakmai irányítás (szakfelügyelet) része. Az ellenőrzés és annak eredményeként kialakított értékelés során alapvető szempont annak vizsgálata, hogy az informatikai szolgáltatások, tevékenységek hogyan járulnak hozzá a szervezet működésének eredményességéhez és hatékonyságához.

Az informatikai ellenőrzés része lehet (nem informatikai) vezetői átfogó, cél- és témaellenőrzéseknek és az informatikai szakmai irányítás részeként a közvetlenül alárendelt, illetve a szakmai irányítás alá tartozó szervezeteknél, szervezeti elemeknél. Az informatikai ellenőrzés kiterjed az informatikai és az alkalmazó szervezetekre, szervezeti elemekre. Magában foglalja az informatikai szolgáltatások igénybevétele, hasznosítása ellenőrzését, az informatikai szaktevékenységek vezetésének és végrehajtásának ellenőrzését, valamint a vezető, alkalmazó és szakállomány felkészültségének ellenőrzését.

Az *informatikai (szak)felügyelet* – a szabályozás és a tervezés mellett – az informatikai szakterületért felelős szervezetek, szervek alapvető eszköze a közigazgatásban, a védelmi szférában, illetve általában az összetett szervezetrendszerekben. Az informatikai (szak)felügyelet az érintett tevékenységek köre alapján tovább tagolható például az informatika-alkalmazás, az informatikai fejlesztések és beszerzések, az informatikai üzemeltetés, az informatikai felkészítés, vagy az informatikai biztonság szaktevékenységei felügyeletére. Az informatikai szakmai felügyelet alapja az informatikai tevékenységek különböző eszközökkel (jelentés-, tájékoztatás-, információkéréssel; ellenőrzéssel; stb.) történő figyelemmel kísérése és szükség esetén intézkedés az előírások betartására. Közvetlen beavatkozásra, intézkedésre jellemzően az alaprendeltetés szerinti (hierarchikus) vezetési struktúra vezetői jogosultak, az informatikai tevékenységért felelős szervnek erre kezdeményezési, javaslattételi jogköre és feladata van (egyes kérdésekben azonban a szabályozás számára közvetlen beavatkozási lehetőséget is biztosíthat).

10. A SZAKTERÜLET, A SZERVEZET SZAKMAI KÉPVISELETE

A *képviselet* jogi értelemben jognyilatkozat megtétele más helyett és más nevében úgy, hogy a képviselt válik jogosítottá és kötelezetté. Köznapi értelemben a képviselet más(ok) nevében történő eljárás, más(ok) helyettesítése. A képviselet alapulhat jogszabályon,

szervezeti viszonyon (belső szabályzat), vagy meghatalmazáson. A szervezetek képviselete általánosságban a vezető, a vezető tisztségviselők feladat- és jogköre.

A *szakterületi képviselet* az adott szakmai irányító szerv feladat- és jogköre, tevékenysége az adott szakterület ügyeiben történő eljárásra, állásfoglalásra. Ez két nagy csoportba sorolható: a szakterület képviselete az adott szervezeten belül, illetve a szervezet egészének képviselete szakmai ügyekben a szervezeten kívül. A képviselet megvalósulhat megbeszéléseken, tárgyalásokon, fórumokon; testületekben, bizottságokban; szakmai szervezetekben, egyesületekben; stb. A képviselet jellegét tekintve lehet rendszeres, vagy eseti. A szervezet képviseletéhez hasonlóan a szakterületi képviselet főbb feladatai a szakterületi vezető személyes feladatát képezik.

Az *informatikai képviselet* tehát az informatikai szakmai ügyekben történő eljárás, állásfoglalás feladat- és jogköre a szervezeten belül és azon kívül. A szervezeten belüli informatikai képviseletre általában döntéselőkészítő, javaslattevő állandó testületekben, feladatvégrehajtásra létrehozott munkacsoportokban, illetve eseti megbeszéléseken lehet szükség. Ezek számos más szervezeti funkcióhoz, szakterülethez kapcsolódhatnak, mint például a tervezés, a fejlesztés és beszerzés, vagy a kiképzés és felkészítés. A védelmi szféra szervezetei esetében a szervezeten kívüli informatikai képviselet főbb színterei közé a magyar közigazgatás, az Európai Unió, az európai szervezetek (NATO, EUROPOL, stb.), a nemzetközi és hazai szakmai (informatikai) szervezetek testületei, bizottságai és munkacsoportjai tartozhatnak.

11. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A fentiekben egy adott csoportosításban feldolgozásra kerültek az informatikai irányítás feladatrendszere összetevőinek vezetéselméleti alapjai, alapfogalmai és egyes informatikai szakterületi sajátosságai. A bennük foglaltak jelentős mértékben lefedik a közigazgatási és védelmi szférabeli informatikai irányító szervek feladatrendszerében a jelenlegi gyakorlat szerint megfogalmazott jogköröket és feladatokat. A feldolgozásból igazából talán csak egyetlen feladattípus maradt ki, amely a szervezeti és működési szabályzatokban általában a "gondoskodik valamiről" kifejezéssel szerepel. Ez azonban megítélésünk szerint kerülendő kellene legyen, mert valójában nem határozza meg az informatikai – vagy más – irányító szerv teendőit és az ehhez rendelkezésre álló jogait.

Mint azt a bevezetőben is megfogalmaztuk, a publikációban foglaltak (esetleges további kutatások utáni pontosításokkal, kiegészítésekkel) segítségül szolgálhatnak informatikai irányító szervek feladatrendszerének meghatározásához, jog- és feladatkörök teljességének elemzéséhez. Az egyes feladatcsoportokat sorra véve végiggondolható, hogy az informatikai irányító szervnek például (a teljesség igénye nélkül):

- milyen tervek kidolgozását kell végrehajtania, vagy koordinálnia, milyen tervekbe kell bedolgoznia informatikai szakterületi feladatokat;
- milyen témakörökben rendelkezik döntési, jóváhagyási, egyetértési, vagy véleményezési jogkörrel;
- milyen témakörökben van felügyeleti, vagy ellenőrzési jogköre és feladata.

Végül a megfogalmazott megállapítások alapul és keretül szolgálhatnak további kutatásokhoz, az egyes informatikai irányítási feladatok (pld. stratégiai tervezés, szabályozás, tervezés, stb.) részletesebb elemzéséhez, részfeladataik meghatározásához, eszközeik és módszereik vizsgálatához.

Felhasznált irodalom

[1] MUNK Sándor: Az informatikai irányítás alapjai. – *Hadmérnök*, 2011 (VI.)/4. (216-223. o.)

[2] *17/2010 (VIII. 31.) KIM utasítás a Közigazgatási és Igazságügyi Minisztérium Szervezeti és Működési Szabályzatáról.*

[3] *9/2011. (II. 15.) NFM utasítás a Nemzeti Fejlesztési Minisztérium Szervezeti és Működési Szabályzatáról.*

[4] *87/2010. HM utasítás a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról.*

[5] *AAP-6 (2010), NATO Glossary of Terms and Definitions (English and French).* – NATO Standardization Agency, Brussels, 2010. 03. 22.

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Nagyné Takács Veronika
ntakacsv@t-online.hu

A NEMZETI KRITIKUS INFORMÁCIÓS INFRASTRUKTÚRÁK VÉDELMÉNEK SZABÁLYOZÁSI ÉS SZERVEZETI KÉRDÉSEI

HELYZETKÉP AZ EU IRÁNYELV 2012-BEN ESEDÉKES FELÜLVIZSGÁLATA ELŐTT

Absztrakt

A kritikus infrastruktúrák – köztük a kritikus információs infrastruktúrák – védelme elméleti és gyakorlati kérdéseinek áttekintése különösen időszerű az Európai Tanács 2008/114/EK Irányelvének 2012-ben esedékes felülvizsgálata előtt.

The theoretical and practical overview of the critical infrastructure including the critical information infrastructure protection is particularly timely before the review of directive 2008/114/EC of the European Council in 2012.

Kulcsszavak: *kritikus információs infrastruktúra, kritikus infrastruktúra védelem nemzeti programja ~ critical information infrastructure, national program for critical infrastructure protection*

1. BEVEZETÉS

A világ legfejlettebb régióiban kialakulóban levő információs (tudásalapú) társadalom alaptétele, hogy az információ (tudás) válik a legfőbb stratégiai erőforrássá. Ebből következően az információt hordozó (létrehozó, tároló, feldolgozó, továbbító) közegek, szervek, szervezetek és személyzetük, valamint mindezek fenntartása és működtetése, irányítása és felügyelete alapvető jelentőségűek a gazdaság fejlődése, a társadalom jóléte és az állam működése szempontjából.

Globalizálódó világunkban nyilvánvaló, hogy nemcsak az információk terjedése/terjesztése válik határtalanná (ide nem értve az üzleti, politikai stb. korlátokat), hanem az információk fenyegetettsége is új dimenziókat kap (például távolról érkező, vagy éppen helyi, váratlan és rendkívül intenzív támadások lehetősége és megvalósulása formájában).

A „minden mindennel összefügg" elvéből következően az információk, az információkat hordozó elemek és eszközök – az információs infrastruktúra – továbbá az információs infrastruktúrákat használó társadalmi, gazdasági és állami szereplők olyan bonyolult egymásra utaltságban léteznek (akár államhatároktól függetlenül), hogy a rendszer bármelyik elemének sérülése vagy kiesése beláthatatlan – kritikus – következményekkel járhat.

Az itt vázolt problémakör elemzése az új évezred első éveiben – a világ különböző pontjain elkövetett terrorcselekmények (New York, Madrid, London) és az informatikai rendszereket ért támadások (Észtország, Litvánia, Egyesült Államok) – után vált intenzívvé, amikortól az államok és a nemzetközi szervezetek komplex, hosszabb távra szóló megoldást kezdtek keresni az átéltekhez hasonló támadások megelőzése, illetve lehetséges hatásaik csökkentése érdekében.

Magyarország folyamatosan együtt haladt az európai törekvésekkel, így a nemzeti és a közösségi eredmények – az állami (közigazgatási) és a tudományos tevékenységet tekintve is – összevethetők.

Érdemes röviden áttekinteni, mi történt eddig, és milyen feladatok vannak előttünk a nemzeti kritikus információs infrastruktúrák védelme terén.

2. A KRITIKUS INFRASTRUKTÚRÁK VÉDELMÉNEK ELMÉLETI MEGALAPOZÁSA

2.1. Fogalmi tisztázás

A *nemzeti kritikus információs infrastruktúrák* kifejezés minden egyes eleme fogalmi tisztázást célzó pontosítások tárgya volt – és az még ma is.

A legegyszerűbbnek tűnik az *infrastruktúrák* meghatározása; e kérdésben viszonylagos konszenzus van a szakirodalomban*: mindazon fizikai létesítmények, eszközök, rendszerek (hálózatok), az ezeket működtető szervezetek és ezek személyi állománya, továbbá az általuk alkalmazott eljárások összessége, amelyet meghatározott társadalmi, gazdasági vagy állami feladat ellátására hoztak létre és működtetnek*. A fogalom meghatározásából két elem – a szervezet és a személyzet – még nem minden definícióban jelenik meg, [1] [2] jóllehet a védelem tervezése és szabályozása során ezeknek is szerepet kell kapniuk. A meghatározásokban több ízben megjelenik a szolgáltatás elem is, [3] [2] ennek szerepeltetése elhatárolási kérdést vet fel az eljárások és az infrastruktúra rendeltetése vonatkozásában.

A *kritikus* jelző tartalmát érintően már nincs ilyen egységes alap. A legáltalánosabb megfogalmazás szerint kritikus az az infrastruktúra, amelynek *működése létfontosságú a társadalom, a gazdaság vagy az állam működése szempontjából*, azaz sérülésének, működésképtelenségének hatása jelentősen túlmutat az infrastruktúra működtetői (és egyes esetekben a felhasználói) körén.

A fenti megfogalmazás konkretizálására három dimenziót (kiterjedés/hatókör, súlyosság/nagyságrend és időbeli hatás) és változó számú elemből álló horizontális szempontrendszert (társadalmi, gazdasági, környezeti, politikai, pszichológiai, közegészségügyi, [4] valamint nemzetbiztonsági, továbbá kölcsönös függőségi [3] hatás alapján történő megkülönböztetést) tartalmaznak a dokumentumok. A legutolsó szempont-elem kicsit megtöri az addigi logikát; az interdependencia nem annyira önálló, inkább az előzőleg említettek súlyosító tényezője.

A dimenziók számszerűsítése – a küszöbértékek meghatározása – már a konkretizálás további lépését jelenti. A hatás földrajzi kiterjedésének meghatározására a globális, nemzetközi, nemzeti, továbbá a nemzetin belül a regionális vagy helyi szint szerinti megkülönböztetés az elfogadott. A súlyosság tekintetében a horizontális szempontok mentén meghatározható mérőszámokban kifejezhető károk nagysága az irányadó. Az időbeliséget az azonnali, 24-48 órás, hetes, éves időtartamban mérhető kiesés/helyreállítás alapján lehet definiálni.

Az *információs* jelző részben ágazati meghatározást takar (lásd később), részben infrastruktúra-jelleget definiál. Haig Zsolt és Várhegyi István rámutat, a különböző rendeltetésű infrastruktúrák között vannak olyanok, amelyek „lehetővé teszik a társadalom valamely információs funkciójának zavartalan működését", azaz „biztosítják az információk megszerzését, előállítását, továbbítását, feldolgozását és felhasználását". Ezeket az információs (és nem szállítási, egészségügyi stb.) rendeltetésű infrastruktúrákat *funkcionális információs infrastruktúrák*nak nevezik, megkülönböztetve azoktól, amelyek egy-egy információs vagy nem-információs (azaz pl. szállítási, egészségügyi stb.) rendeltetésű infrastruktúra működtetésében informatikai („kutató, fejlesztő és ellátó") eszközrendszerként közreműködnek (*támogató információs infrastruktúrák*). [5] A megkülönböztetés megalapozottságát elismerve jelezni szükséges, hogy a közigazgatási tipológiában a tevékenységek jellegének meghatározásakor a funkcionális jelző a támogató jellegű tevékenységet jelöli, szemben a szakmai jelzővel meghatározott alaptevékenységgel. [6]

Az *információs* jelző kapcsán egy hazai sajátosságra is ki kell térni. Az angol *information infrastructure* kifejezésnek két magyar fordítása is létezik: *információs* illetve *informatikai infrastruktúra*. Több szerző foglalkozik a két kifejezés elkülönítésével, aminek lényege, hogy az előbbin az információt (mint adatot, tudást) tartalmazó rendszert, hálózatot stb. értik, utóbbin magát az informatikai (számítástechnikai-elektronikai-elektronikus stb.) (eszköz)rendszert. [1] [7] A 2010-ben közzétett kormányzati stratégiai dokumentum [8] az előbbi, a 2009-ben, 2011-ben közzétett EU bizottsági közlemények [9] [10] magyar fordítása az utóbbi kifejezést alkalmazza. Megfontolandónak tűnik az utóbbi kifejezés elfogadása, mivel így az informatikai közmű – Munk Sándor kifejezésével: az „információs szolgáltatásokat nyújtó technikai hálózat" [7] – és a benne kezelt, tárolt, továbbított információtartalom mind elméleti, mind szabályozási szinten elkülöníthető. Ezt a megközelítést erősítik a kritikus infrastruktúrák informatikai rendszerek általi meghatározottságáról szóló megállapítások is. [11]

A *nemzeti* jelzőnek elsősorban az Európai Unió kritikus infrastruktúrákkal kapcsolatos tevékenységével összefüggésben van jelentősége. A szubszidiaritás elve alapján európai kérdéssé az a probléma válhat, amelynek megoldására a tagállami, azaz nemzeti keretek nem elegendőek. A kritikus infrastruktúrák esetében európainak minősül minden, „a tagállamokban található olyan kritikus infrastruktúra, amelynek megzavarása vagy megsemmisítése jelentős hatással lenne legalább két tagállamra". [12] Ebből következően a kritikus (információs) infrastruktúrák esetében elsődleges a nemzeti szintű megközelítés (meghatározás, azonosítás és védelem), és csak ezt követheti a nemzeti szinten túlnyúló, európai szintű védelem megvalósítása.

Az európai megközelítést Précsényi Zoltán és Solymosi József két tanulmánya részletesen elemzi, [13] [14] és a nemzeti feladatvállalást erősítő következtetésre jut: „a Bizottságnak adott, európai kritikus infrastruktúra-védelmi rendszer megalkotására irányuló mandátummal egyidőben minden tagállam megvizsgálta saját nemzeti rendszereit, s megállapította, hogy ha nem is a "kritikus infrastruktúrák" újszerű terminológiája alatt, de régóta van saját, bejáratott és működő védelmi rendszere, amely egyfelől szuverén stratégiai érdekeken alapul, másfelől pedig közigazgatási, politikai és ezer egyéb oknál fogva összeegyeztethetetlen a többi tagállamban honos rendszerekkel, szemléletekkel". [14]

2.2. Azonosítás és kijelölés

A fogalom kidolgozását az egyes kritikus infrastruktúrák azonosításának kell követnie. Az azonosítás jelenleg azon ágazatok és alágazatok számbavételénél tart, amelyek kritikus infrastruktúrákkal rendelkeznek vagy rendelkezhetnek. A kiválasztási szempontok és a már jelzett horizontális szempontrendszer között nyilvánvalóan és szükségszerűen szoros kapcsolat van. Az egyes államok – hagyományaik, közigazgatási berendezkedésük stb. alapján – eltérő csoportosítást alkalmaznak; tradicionálisan megnevezett szektorok az energiaellátás, közlekedés, távközlés, egészségügy, élelmiszer- és vízellátás, pénzügy, közbiztonság.

Az ágazatok és alágazatok azonosítását követő lépés a kijelölés kell, hogy legyen: azaz a konkrét infrastruktúrák és infrastruktúra-elemek (intézmények, rendszerek, hálózatok stb.) meghatározása. A probléma bonyolultságát szemléletesen mutatja a Bush-adminisztráció 2002-ben tett megállapítása: „a különböző kritikus infrastruktúra szektorokon belüli egyes eszközök, feladatok és rendszerek nem azonosan fontosak ... a közlekedési szektor létfontosságú, de nem minden egyes híd kritikus jelentőségű a Nemzet egésze számára". [15] Ahogyan Bukovics István és Vavrik Antal írja: „ami kritikus helyileg, az nem biztos, hogy kritikus az állam számára is. Ráadásul, erről gyakran még pontos információ sincs, hiszen jellemzően területi, vagy helyi szinten nem rendelkeznek szakszerű, tudományosan megalapozott kockázatértékeléssel." [16] Ezen kívül a kritikusság ismérve – ahogyan a fogalmi tisztázás kapcsán már látható volt – térbeli, horizontális és időbeli tényezők módosulása okán folyamatosan változik.

2.3. Védelem

A fogalmi tisztázás, az azonosítás és a kijelölés nem öncélú: a helyzetfelmérés célja a megfelelő védelem megtervezéséhez és megvalósításához szükséges elvi és gyakorlati alapadatok meghatározása.

A védelem tervezése során tisztában kell lenni azzal a (többször bebizonyosodott) ténnyel, hogy teljes körű védelem nincs. A védelem szintje, eszközrendszere tökéletes nem, legfeljebb optimalizált (kockázatarányos, fenntartható, költséghatékony stb.) lehet.

Tekintettel kell lenni a fenyegetések típusára és az egyes fenyegetési típusokhoz tartozó események bekövetkezésének valószínűségére. Az elsődleges csoportosításhoz támpontot adhat például Nagy Rudolf tipológiája, amely alapján a zavar, a sérülés forrása lehet technológiai rendellenesség (pl. anyagszerkezeti hiba), külső – természeti – tényező kiváltotta véletlen baleset (pl. természeti katasztrófa) és szándékolt kár (pl. terrortámadás, szabotázs). [17] A zavar jelentkezhet közvetlen vagy közvetett módon is. Az információs rendszerek kapcsán Haig Zsolt és Várhegyi István a konfliktushelyzetek, a technikai lehetőségek és a motivációk (politikai, gazdasági, pénzügyi, katonai, szociális stb. célok) szerint változó fenyegetéseket különböztet meg. [5] Muha Lajos a fizikai és az információs dimenzióból érkező fenyegetéseket különíti el, ez utóbbi csoporton belül a támadó személye (alkalmazott, terrorista stb.) és az elkövetés módja (adathalászat, rosszindulatú programok bejuttatása, elektronikai felderítés stb.) szerint példálózó felsorolást is ad. [1]

A két utóbb említett csoportosítás az információs infrastruktúrák fenyegetettségének egy sajátosságára is felhívja a figyelmet: ezen infrastruktúrák vonatkozásában a fenyegetések, támadások nem feltétlenül a működés megzavarására, az infrastruktúra megsemmisítésére irányulnak, a cél lehet az információtartalom megismerése, ellenőrzés alatt tartása is. A kritikus információs infrastruktúrák elleni támadások módszereit (számítógép-hálózati támadás, elektronikai felderítés és elektronikai támadás) és eszközeit részletesen elemzi Haig Zsolt, Hajnal Béla, Kovács László, Muha Lajos és Sík Zoltán Nándor közös tanulmánya. [18]

A fenyegetéseknek, a kritikus infrastruktúrák sebezhetőségének és a megzavarásuk vagy megsemmisítésük okozta károk lehetséges hatásainak felmérése – a kockázatelemzés – adja a kiindulópontot a védelem megtervezéséhez és megvalósításához.

A fentiek alapján határozhatók meg a védelem céljai is: az infrastruktúrák működésében fellépő zavarok megelőzése, a zavarok elhárítása és a rendeltetésszerű működés helyreállítása. A bekövetkező károk oldaláról: a károk megelőzése, a károk enyhítése, illetve az eredeti állapot helyreállítása. A szándékolt károk (támadások) veszélyének jelentőségét mutatja, hogy a megelőzés – elhárítás – helyreállítás (alapvetően működési szempontú) hármas célján túl Muha Lajos hangsúlyt helyez a támadók elrettentésére, azonosítására, elfogására (és nyilvánvalósan: felelősségre vonására) is. [1]

A védelem tervezésénél törekedni kell arra, hogy minél több szempont számbavételével történjék meg a védelmi rendszer kialakítása.

A védelmi rendszer legyen többszintű és többféle elemből álló. A nemzetközi és a hazai szabványok, legjobb gyakorlatok a szervezeti és személyi, fizikai (környezeti), informatikai és adminisztratív védelmi eszközök, eljárások komplex rendszerét javasolják, amelyben a helyi és a központi feladatok, felelősségi körök összhangja is megvalósul.

A szakma által ismert és alkalmazott fenti szempontrendszer néhány eleme már működő evidencia (pl. a helyi szintű objektumvédelem, amely magában foglalja az őrzésvédelmet, tűzvédelmet, vagyonvédelmet stb., mindezt személyi és biztonságtechnikai elemek belső szabályozókban előírt, kombinált alkalmazásával), mások még csak problémafelvetések. Ez utóbbi körbe sorolható a központi és a helyi, az állami és az önkormányzati, illetve a kormányzati és az üzemeltetői felelősség meghatározása és a terhek megosztása, vagy éppen a nemzeti szabályrendszer és nyilvántartás/számontartás kialakítása és működtetése.

A feladatok, a felelősségek és a terhek megosztása a kormányzati és az üzemeltetői szint között kiemelt jelentőségű. A kritikus infrastruktúrák üzemeltetői (tulajdonosai) gyakran nem állami, hanem piaci szereplők, az ügyfelek viszont az állam polgárai. A kritikus infrastruktúrák kieséséből, megsemmisüléséből keletkező károk nemcsak az üzemeltetőknek okozhatnak veszteséget, hanem az embereket mint ügyfeleket és mint az infrastruktúra környékén élő lakosságot is sújthatják. Ez utóbbi esetek okán az államnak nyilvánvaló kötelezettsége a kármegelőzés és a kárenyhítés. A kritikus infrastruktúrák jelentőségére tekintettel az államnak az is érdeke, hogy az üzemeltetésben közreműködő piaci szereplők érdekeltsége is megmaradjon. A piaci szereplők oldaláról vizsgálva a kérdést leszögezhető, hogy az üzemeltetés mint profittermelő tevékenység része kell legyen a védelmi intézkedések megtervezése és megvalósítása is. A védelemnek pedig komoly költségei vannak. Mindezekből következően a kormányzati és a piaci szereplők egymásra vannak utalva, és előremutató megoldás csak akkor tud születni, ha abban mindkét oldal érdekei érvényesülnek.

A védelem központi (állami) szabályozásának, valamint irányításának, felügyeletének és ellenőrzésének szükségessége – a meghatározások alapján – vitathatatlan. A megvalósítást tekintve még van teendő.

3. EURÓPAI UNIÓS EREDMÉNYEK A KRITIKUS INFRASTRUKTÚRÁK VÉDELME TERÉN

3.1. Általános iránymutatás és együttműködés

Mind az eddig tárgyalt elméleti kérdések, mind az ezután említendő gyakorlati eredmények – tagságunkból fakadóan magától értetődően – szoros kapcsolatban voltak és vannak az Európai Unió kritikus infrastruktúrákat érintő tevékenységével.

Az Európai Unió Tanácsa 2004-ben kérte fel a Bizottságot, hogy készítsen átfogó stratégiát a kritikus infrastruktúrák védelmére. 2005-ben a Bizottság *Zöld Könyv*et fogadott el a kritikus infrastruktúrák védelmére vonatkozó európai programról, [19], majd 2006-ban javaslatot dolgozott ki egy tanácsi irányelvre, [4] [20] amelyet az Európai Unió Tanácsa 2008-ban fogadott el. [12]

Az irányelv közös eljárást hozott létre az európai kritikus infrastruktúrák (European critical infrastructure, ECI) azonosítására és kijelölésére, valamint közös megközelítést alakított ki annak értékelésére, hogy szükséges-e az érintett infrastruktúrák védelmét javítani. Célul tűzte ki a bizalmon és biztonságon alapuló, strukturált és következetes információcsere megvalósítását az ECI-k tulajdonosai/üzemeltetői és a tagállam, valamint az egyes tagállamok, továbbá a tagállamok és a Bizottság között. Az ECI-k azonosítása és kijelölése érdekében meghatározta azok fogalmát,

rögzítette a horizontális kritériumokat (a küszöbértékek meghatározását a tagállamokra bízva), kijelölte azokat az ágazatokat és alágazatokat, amelyek európai kritikus infrastruktúrával rendelkezhetnek. A tagállamoknak kötelezte arra, hogy 2011. január 12-éig jelöljék ki az ECI-ket az energia- és a közlekedési ágazatban. Jelezte továbbá, hogy az irányelv (2012. január 12-étől előírt) felülvizsgálata és a további ágazatok meghatározása során elsőbbséget kell biztosítani az IKT – információs és kommunikációs technológiák – ágazatnak.

3.2. Információbiztonsági együttműködés és cselekvési terv

Az együttműködés általános kereteinek kidolgozásán túl a Bizottság a Tanácstól kapott felhatalmazás alapján 2008-ban javaslatot dolgozott ki a kritikus infrastruktúrák figyelmeztető információs hálózatának (Critical Infrastructue Warning Information Network, CIWIN) létrehozására is. [21] A Bizottság javaslatában megállapította, hogy az Európai Unióban számos ágazati sürgősségi riasztórendszer létezik, de ágazatokat átfogó jellegű nincs, ezért egy biztonságos, önkéntes és többszintű kommunikációs/riasztórendszer létrehozását indítványozta, két elkülönült – „sürgősségi riasztórendszer és a kritikus infrastruktúrák védelmével kapcsolatos vélemények és bevált módszerek cseréjére szolgáló elektronikus fórum” – funkcióval.

A „Közösségen belüli magas szintű és hatékony hálózat- és információbiztonság biztosítása”, valamint a „hálózat- és információbiztonsági kultúra kifejlesztése” érdekében az Európai Parlament és a Tanács létrehozta az Európai Hálózat- és Információbiztonsági Ügynökséget (European Network and Information Security Agency, ENISA), meghatározta feladatait, szervezetét és működési rendjét. [22] Az ENISA információcserét, együttműködést lehetővé tevő és koordináló, tanácsadó feladatokat is ellátó szervezetként jött létre öt éves időtartamra. 2009-ben megbízatási idejét 2012. március 13-áig meghosszabbították. [23] 2010-ben a Bizottság az ENISA megerősítésére és modernizálására, továbbá tevékenysége további öt évre történő meghosszabbítására vonatkozó rendelettervezetet készített, mivel „szükség van egy olyan szakpolitikai eszközrendszerre, amely proaktív módon képes azonosítani a hálózat- és információbiztonság területén jelentkező kockázatokat és rendszereink gyenge pontjait, amely létrehozza a válaszadás mechanizmusait, és amely képes

gondoskodni arról, hogy ezeket a válaszadási mechanizmusokat az érdekeltek ismerjék és alkalmazzák". [24]

Az információcserén és a koordináción túl az Európai Unió *Cselekvési terv*et is készített [9] és annak végrehajtását is figyelemmel kíséri. [10] A *Cselekvési terv* öt pillére a Felkészülés és megelőzés, az Észlelés és reagálás, a Hatások enyhítése és a helyreállítás, a Nemzetközi együttműködés és az Európai kritikus infrastruktúrákra vonatkozó követelmények az IKT-ágazat számára. Az utóbbi kérdéskör kapcsán a 2011-es közlemény rögzíti, hogy elkészült a vezetékes és mobiltávközlésre, valamint az internetre vonatkozó kritériumrendszer tervezete, az IKT-ágazatspecifikus kritériumok műszaki vitáját 2011 végén tervezik lezárni, konzultációkat terveznek a magánszférával az ágazati kritériumokról és a Bizottság megtárgyalja a tagállamokkal a 2008/114/EK irányelv 2012-ben esedékes felülvizsgálata során megfontolandó elemeket is. [10]

4. GYAKORLAT: A KRITIKUS INFRASTRUKTÚRÁK VÉDELMÉVEL KAPCSOLATOS SZABÁLYOZÁS ÉS SZERVEZETRENDSZER

4.1. Elvi keretek, programok: országgyűlési és kormányhatározatok, stratégiai dokumentumok

A kritikus infrastruktúrák (köztük a kritikus információs infrastruktúrák) védelmének céljait, irányait, kereteit, továbbá a védelemmel kapcsolatos kormányzati feladatokat országgyűlési és kormányhatározatok, továbbá különböző stratégiai dokumentumok rögzítik.

Az Országgyűlés 1998-ban fogadta el a *Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről* szóló határozatot, amely a biztonságot átfogó módon értelmezi, és fogalmába beleérti annak „információs és technológiai dimenzióját" is. [25]

A határozat alapján dolgozta ki és fogadta el a kormány a *Magyar Köztársaság nemzeti biztonsági stratégiáját*, amely a terrorizmus elleni küzdelem keretein belül szól a kritikus infrastruktúrák védelmének szükségességéről, *Az információs társadalom kihívásai* alfejezetben pedig leszögezi „az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is", és szoros koordinációt ír elő „mind a szövetségesekkel, mind az informatikai és távközlési szolgáltatók, valamint kutatóközpontok között". [26]

2004 és 2007 között három kormányhatározat született a terrorizmus elleni küzdelem aktuális feladatairól, amelyek az *Európai Unió Terrorizmus Elleni Cselekvési Terv*ének hatékony végrehajtása érdekében a kritikus infrastruktúrák védelmével kapcsolatos ágazatközi koordinációs feladatokat határoztak meg. [27] [28] [29]

Szintén az európai folyamatokat képezte le az a 2008-ban közzétett kormányhatározat, amelynek 1. sz. melléklete a *Zöld Könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról*, 2. sz. melléklete a *Szektorok és felelősök listája*. [3] A *Zöld Könyv* a kritikus infrastruktúrák meglehetősen tág, a kölcsönös függőséget hangsúlyozó meghatározását adja, azonban a kritikus információs infrastruktúrák definíciójával – ellentétben az európai *Zöld Könyv*vel – adós marad. Tartalma értelemszerűen szoros kapcsolatot mutat az európai *Zöld Könyv*vel, az alapfogalmak leírásán túl meghatározza a védelem céljait és alapelveit, iránymutatást ad a kritikus infrastruktúrák kijelöléséhez, rögzíti a védelemben részes szereplők feladatait és felelősségét, együttműködési formáit. A *Szektorok és felelősök listája* felsorolja az érintett ágazatokat és alágazatokat; a kritikus információs infrastruktúrákat a kilenc alágazatot tartalmazó infokommunikációs technológiák ágazat képviseli.

Az Európai Unió Tanácsa által meghatározott feladatok teljesítése érdekében 2010-ben újabb kormányhatározat született. [30] A dokumentum az ECI-k védelmével kapcsolatos koordinációs feladatok ellátására nemzeti kapcsolattartó pontként (European Critical

Infrastructure Protection Contact Point) a belügyminisztert jelöli ki, munkacsoportot hoz létre az ECI-k azonosításához szükséges kritériumrendszer kidolgozására (2011. január 5-ei határidővel) és az ECI-k kijelölésére vonatkozó javaslat megfogalmazására, az ECI-k kijelölésével a nemzeti fejlesztési minisztert bízza meg (2011. február 15-ei határidővel), rendelkezik az Európai Bizottság felé fennálló jelentési kötelezettség teljesítéséről (első alkalommal 2011. január 12-ei határidővel).

Ez a kormányhatározat az európai uniós teendőkön túl a nemzeti kritikus infrastruktúrák védelmével kapcsolatos feladatokat is rögzít, így az említett munkacsoportot bízza meg a nemzeti kritikus infrastruktúra védelem intézmény- és kritériumrendszerének kidolgozásával, továbbá a kormányzati szereplők és a civil szféra kritikus infrastruktúra védelemmel kapcsolatos együttműködésének megteremtése érdekében konzultációs fórum felállítását rendeli el (2011. március 31-ei határidővel). A dokumentum külön hangsúlyt helyez a honvédelmi érdekből kritikus infrastruktúrák védelmére: a honvédelmi minisztert felhívja a vonatkozó intézmény- és követelményrendszer kidolgozására (2011. február 28-ai határidővel).

2011. február 2-ai keltezésű a tárgyban közzétett legutóbbi kormányhatározat. [31]

A kritikus információs infrastruktúrák védelmét önálló alfejezetben tárgyalja az egyik legutóbbi, a Nemzeti Fejlesztési Minisztérium által készített stratégiai dokumentum. [8] A szakmai műhelyek által kidolgozott, valamint a nemzeti *Zöld Könyv*ben megjelent elméleti megközelítés rövid áttekintése után négy akcióban foglalja össze a tennivalókat, amelyek lényege a központi (állami) szerepvállalás növelése a védelem vezetésében és a védelmi stratégia kidolgozásában, a nemzeti és az európai kritikus infrastruktúrák kijelölésében és a kijelölések felülvizsgálatában, a feladat-meghatározásban és a szabályozásban, továbbá összkormányzati szinten a tudatosság növelése, az oktatás és a képzés.

4.2. Ágazati jogszabályok

A stratégiai jellegű, programadó dokumentumokon túl meghatározó jelentőségűek az egyes ágazatokra vonatkozó jogszabályok. Ezek már jóval a kritikus infrastruktúrák fogalmának megjelenése előtt stabil alapot képeztek az egyes szektorok tevékenységéhez, beleértve a védelmi feladatokat is. Igaz ez a kritikus információs infrastruktúrák esetében is. Sőt, a kritikus infrastruktúrák első hazai normatív megfogalmazását egy ágazati védelmi jogszabály tartalmazza. [32]

Az ágazati jogszabályok – törvények, kormány- és miniszteri rendeletek – számbavétele meghaladná jelen munka kereteit.

A kritikus információs infrastruktúrák vonatkozásában a legjelentősebb jogszabályok az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.) [33] és végrehajtási rendeletei, így különösen a *223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról*. [2] Ez utóbbi rögzíti, hogy az elektronikus közszolgáltatások nyújtását, illetve igénybevételét támogató központi informatikai és kommunikációs rendszerek együttese, azaz „*a központi rendszer – a kritikus infrastruktúra része*, védelmét a kritikus infrastruktúrára vonatkozó, nemzetközileg kialakult biztonsági követelményeknek megfelelően kell kialakítani”. [2] A jogszabály meghatározza a kritikus infrastruktúra és az információbiztonsági fenyegetés fogalmát, minőségirányítási, biztonsági, szabályozási és ellenőrzési követelményeket fogalmaz meg, rendelkezik az informatikai biztonság irányításáról és a működtetéssel kapcsolatos felelősségi viszonyokról. Bár a rendelet csak az elektronikus közszolgáltatás vonatkozásában szabályoz(hat), előírásai – némi fogalmi pontosítás után – irányadóak lehetnek általánosabb szabályozás esetében is. A dokumentum kétségtelen érdeme, hogy a korábban csak legjobb gyakorlatként illetve szabványokban megjelenő informatikai biztonsági előírásokat normatív szintre emelte. A jogszabály rendelkezik a Nemzeti Hálózatbiztonsági Központ létrehozásáról is (lásd később).

4.3. Új megközelítés: az adatvagyon törvény

A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény (Nav. tv.) [34] és végrehajtási rendelete [35] adatvédelmi okokból – tehát nem az infrastruktúra védelme érdekében – rögzít a közigazgatásban végzett elektronikus adatfeldolgozásra vonatkozóan biztonsági előírásokat. Ezek az előírások meghatározzák a védendő adatállományt kezelő informatikai rendszerek elvárt védelmi szintjét (*Korlátozott terjesztésű* minősítési szintű adatot kezelő rendszerre egyébként irányadó személyi, fizikai, adminisztratív és elektronikus biztonsági követelmények teljesítése), illetve korlátozzák ezen rendszerek működtetőinek körét (csak államigazgatási szerv vagy kizárólagos állami tulajdonú gazdálkodó szervezet lehet). A korábban kifejtettek alapján ezek a rendelkezések a kritikus információs infrastruktúrák egy típusára vonatkozó konkrét védelmi intézkedéseknek is tekinthetők.

4.4. Szervezetrendszer

A közigazgatás szervezetrendszerén belül az érintett szereplők, feladataik, felelősségeik, együttműködési formáik – az előbbiekben tárgyalt stratégiai-koordinációs illetve ágazati-operatív szinten – azonosíthatók.

A már idézett, 2010-ben közzétett kormányhatározat két új együttműködési fórum kialakításáról rendelkezett. A (korábban már említett) közigazgatási munkacsoport létrehozására a belügy-, a nemzeti fejlesztési, a nemzetgazdasági, a közigazgatási és igazságügyi és a honvédelmi minisztert hívta fel, a kormányzat és a civil szféra közötti együttműködés megteremtésére az érintett miniszterek részéről kijelölt vezetők, valamint az infrastruktúra-tulajdonosok, üzemeltetők, érdekvédelmi szervezetek, tudományos testületek bevonásával konzultációs fórum működtetését írta elő. [30]

A kritikus információs infrastruktúrák védelmében meghatározó szerepet játszó Nemzeti Hálózatbiztonsági Központ (NHBK) tevékenységének előzményei 2004-re nyúlnak vissza, amikor a Puskás Tivadar Közalapítvány (PTA) az Informatikai és Hírközlési Minisztérium támogatásával programot indított egy magyarországi hálózatbiztonsági központ létrehozása érdekében. [36] A PTA-CERT Hungary Központ 2005. januártól kezdte meg működését a Miniszterelnöki Hivatal Elektronikuskormányzat-központ felügyelete alatt, 2010. január 1-jétől – a már idézett kormányrendelet alapján, „a magyar kritikus információs infrastruktúrák védelme, valamint a központi rendszeren megvalósuló kommunikációs biztonság, a vírus- és más támadások káros hatásainak korlátozása érdekében nemzetközi együttműködéssel” – az NHBK feladatait is ellátja, továbbá magyar Nemzeti Kapcsolattartó Pontként (NKP) és kormányzati számítástechnikai sürgősségi reagáló egységként (kormányzati CERT) működik. [2] Ez utóbbi minőségében együttműködést folytat más nemzeti (német, holland, lengyel stb.) és nemzetközi CERT szervezetekkel (Forum of Incident Response and Security Teams, FIRST, European Government CERTs group, EGC).

4.5. Hazai szakmai - tudományos eredmények

A kritikus infrastruktúrák és a kritikus információs infrastruktúrák védelmével foglalkozó (az előzőekben többször idézett) szakértői kör az elmúlt években az elméleti kérdések vizsgálatán túl tevékeny szerepet vállalt a kormányzati jogalkotás és jogalkalmazás támogatásában is. Az ismertetett tudományos publikációk, stratégiai dokumentumok és jogszabályok kevés különbséggel ugyanazon gondolatmenetet tükrözik, viszonylag egységes kiindulási pontot biztosítva a gyakorlati megvalósításhoz.

A tudományos tevékenység a fogalmi tisztázáson túl módszertani alapot is kívánt nyújtani a kritikus infrastruktúrák kijelöléséhez és azonosításához, [1] [18] sőt egyes információs infrastruktúrák esetében konkrét rendszerek elemzéséig is eljutott. [37] A módszertani javaslatok a már ismertetett elméleti alapvetésből kiindulva igyekeznek konkretizálni az

azonosítás és kijelölés folyamatát. Azon ágazatok meghatározása, amelyek kritikus infrastruktúrákkal rendelkezhetnek – különösen az EU és a nemzeti *Zöld Könyv* ismeretében – egyszerű feladatnak tűnik. Megjegyzendő, hogy éppen az információs infrastruktúrák területe az, ahol már az alágazatok elhatárolása is problémát okoz. Muha Lajos külön alágazatként nevesíti az informatikai rendszerek és hálózatok, valamint a közigazgatási informatika és kommunikáció területét, továbbá négy távközlési területet, vegyítve az infrastruktúra-jelleg és a rendeltetés fogalmát. [1] Ugyanez a csoportosítás jelenik meg némi módosítással a nemzeti *Zöld Könyv*ben is. [3] A kritikusság értékelése minőségi és mennyiségi jellemzőkön alapulhat. Többször idézett alaptétel, hogy a nemzeti szempontból kritikus és a helyi szinten kritikus fogalma nem esik egybe. A megkülönböztetéshez segítséget nyújthat a számszerűsítés: a javaslat megfogalmazói – külföldi példa alapján – a küszöbértékeket egy háromfokozatú skála (alacsony - közepes - magas) szerint határoznák meg. [18] Az ilyen típusú kategorizálás szolgálhat alapul a kritikus infrastruktúrák kijelöléséhez és rangsorolásához. A végeredményt minőségi (nem mérhető vagy pontosan nem mérhető) jellemzők is befolyásolhatják. Ez utóbbi körbe tartozik az államba vetett bizalom megrendülése, az állampolgárok társadalmi-politikai környezethez viszonyulása (az Egyesült Államokban 2003-ban kiadott elnöki direktíva – morális jelentőségükre tekintettel – a nemzeti emlékműveket és szimbólumokat is a nemzeti kritikus infrastruktúrák körébe sorolja). [39] További pontosítást eredményezhet a kölcsönös függőségi mutató, vagyis az tény, hogy egy adott infrastruktúra kiesése kihat-e, és ha igen, mennyiben, további egy vagy több infrastruktúra működésére. Végül pedig a kialakult sorrendet egy új horizontális elem, vagy a dimenziókban bekövetkező módosulás felülírhatja.

A szakértők a kormányzati, társadalmi és gazdasági szereplőknek a kritikus infrastruktúrák védelmével kapcsolatos feladatait is számba vették. Kovács László 2008-ban írt, kormányzati feladatokat áttekintő tanulmányának megállapításai ma is időszerűek. [38] A feladatok meghatározása és végrehajtása tekintetében kettősség tapasztalható: az egyes szektorok tradicionálisan vagy jól felfogott gyakorlati érdekből rendelkeznek stratégiával, szervezetrendszerüket, tevékenységüket, együttműködésüket leíró és keretbe foglaló jogszabályokkal, működésük feltételeit meghatározzák és igyekeznek teljesíteni (teljesíttetni) is – a rendszer működik. Az ágazatok közötti és feletti szintet azonban – egyelőre – a sokszereplős koordinációs fórumok jelentik. Márpedig a téma jelentőségére tekintettel az ennél határozottabb – az érintettek konszenzuson alapuló véleményét tükröző –, központi szabályozás, a felelősségi körök nemzeti szintű elhatárolása, az irányításhoz szükséges szakmai kompetencia és a pontos feladat- és hatáskör-meghatározás is szükséges lehet.

5. ÖSSZEGZÉS

A kritikus infrastruktúrák (köztük a kritikus információs infrastruktúrák) védelmének tervezése és megvalósítása során alapvető jelentőségű elv az egységesítés és az ágazatfelettiség.

A hazai és a külföldi dokumentumok, jogszabályok, szabványok, ajánlások, tudományos publikációk nyomán a fogalomrendszer egységesíthető. A normatív keretrendszer megalkotása és a már létező jogszabályok felülvizsgálata, egységesítése és kiegészítése az egyik első lépés lehet a kritikus infrastruktúrák védelmének kormányzati feladatai között. A (végre) konzisztens és kötelező fogalomrendszer alapján, a jogszabályban (részben már) rögzített szervezetrendszer és eljárásrend keretein belül biztosított lehet a részletes feladat-meghatározás és -elhatárolás a közigazgatás, a piaci szféra és a társadalmi szereplők számára.

A kritikus infrastruktúrák azonosítása és rangsorolása, majd az eredmények folyamatos aktualizálása a kijelölt kormányzati felelős rendszeres egyeztetést igénylő – nem könnyű – feladata lehet.

Ezt követheti a védelem központi szervezési feladatainak kiteljesítése a már ismertetett elvek szerint.

Ami újszerű: az egységes szemléletmód és megközelítés, az ezen alapuló elemzés és összehasonlítás, az azonos elvek és módszertanok szerinti tervezés és végrehajtás kívánalma.

A „mi és mennyire kritikus infrastruktúra” kérdésre adandó válasz megfogalmazásához minőségi és mennyiségi jellemzők ismerete, közigazgatási és piaci számítások elvégzése és nem utolsósorban az érintettek szakmai alapú konszenzusa szükséges. A „hogyan védjük” kérdésre pedig a már létező eredmények felmérésén, összehasonlításán, szintetizálásán, jobbításán keresztül adható megnyugtató válasz.

Mindez nagy kihívás: túl kell lépni évtizedes hagyományokat és beidegződéseket, újra kell gondolni a saját és a közös értékeket és érdekeket, újfajta – még nem ismert vagy nem elterjedt – módszereket, eljárásokat kell kialakítani és meghonosítani, ráadásul egy sokszereplős – kormányzati és civil, nemzeti és nemzetközi – együttműködés keretében.

Felhasznált irodalom

[1] Muha Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme. Doktori (PhD) értekezés. Budapest, 2007

[2] 223/2009. (X. 14.) Korm. rendelet az elektronikus közszolgáltatás biztonságáról

[3] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

[4] Javaslat - a Tanács irányelve az európai létfontosságú infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (COM (2006) 0787 végleges), 2006. december 12.

[5] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

[6] Magyary Zoltán Közigazgatás-fejlesztési Program (MP 11.0), Közigazgatási és Igazságügyi Minisztérium, Budapest, 2011. június 10.

[7] Munk Sándor: Információs szolgáltatásokat nyújtó hálózatok alapjai – Hadmérnök, 2011. (VI.)/2., 227-243. o. http://www.hadmernok.hu/2011_2_munk.php; (2011. 11. 22.)

[8] Digitális Megújulás Cselekvési Terv 2010-2014., Nemzeti Fejlesztési Minisztérium, Budapest, 2010.

[9] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: a felkészültség, a védelem és az ellenálló képesség fokozása” (COM (2009) 149 végleges), 2009. március 30.

[10] A Bizottság Közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a kritikus informatikai infrastruktúrák védelméről – „Eredmények és következő lépések: a globális kiberbiztonság felé” (COM (2011) 163 végleges), 2011. március 31.

[11] Munk Sándor – Fleiner Rita: Adatbázisok kritikus infrastruktúrákban – Hadmérnök, 2009. (IV.)/1., 225-234. o. http://www.hadmernok.hu/2009_1_fleiner.php; (2011. 11. 22.)

[12] A Tanács 2008. december 8-i 2008/114/EK Irányelve az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (EGT-vonatkozású szöveg), 2008. december 8.

[13] Précsényi Zoltán – Solymosi József: Úton az európai kritikus infrastruktúrák azonosítása és hatékony védelme felé – Hadmérnök, 2007. (II.)/1., 227-243. o. http://www.hadmernok.hu/archivum/2007/1/2007_1_precsenyi.html; (2011. 11. 22.)

[14] Précsényi Zoltán – Solymosi József: Kritikus infrastruktúrák azonosítása: körkép az EU-ban és az USA-ban tapasztalható nehézségekről – Hadmérnök, 2008. (III.)/1., 59-67. o. http://www.hadmernok.hu/archivum/2008/1/2008_1_precsenyi.html; (2011. 11. 22.)

[15] The President's National Strategy for Homeland Security, 2002. július 16. Idézi: Précsényi Zoltán – Solymosi József: Kritikus infrastruktúrák azonosítása: körkép az EU-ban és az USA-ban tapasztalható nehézségekről – Hadmérnök, 2008. (III.)/1., 59-67. o.

[16] Bukovics István – Vavrik Antal: Infrastruktúrák kockázata és biztonsága: kritikai problémaelemzés – Hadmérnök, 2006. (I.)/3. http://www.hadmernok.hu/archivum/2006/3/2006_3_bukovics.html; (2011. 11. 22.)

[17] Nagy Rudolf: A kritikus infrastruktúra védelme és katasztrófavédelmi aspektusai a terrorizmus tükrében – Kard és toll 2006/3., 56-64. o.

[18] Dr. Haig Zsolt - Hajnal Béla - Dr. Kovács László - Dr. Muha Lajos - Sík Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Advisory Kft., 2009.

[19] Zöld Könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról (COM (2005) 0576 végleges), 2005. november 17.

[20] A Bizottság közleménye – A létfontosságú infrastruktúrák védelmére vonatkozó európai programról (COM (2006) 0786 végleges), 2006. december 12.

[21] Javaslat - a Tanács határozata a létfontosságú infrastruktúrák figyelmeztető információs hálózatáról (COM (2008) 0676 végleges), 2008. október 27.

[22] az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról (EGT-vonatkozású szöveg), 2004. március 10.

[23] az Európai Parlament és a Tanács 1007/2008/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló 460/2004/EK rendeletnek az Ügynökség megbízatási ideje tekintetében történő módosításáról (EGT-vonatkozású szöveg), 2008. szeptember 24.

[24] Javaslat – Az Európai Parlament és a Tanács rendelete az Európai Hálózat- és Információbiztonsági Ügynökségről (ENISA) (COM (2010) 521 végleges), 2010. szeptember 30.

[25] 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről

[26] 2073/2004. (IV. 15.) Korm. határozat a Magyar Köztársaság nemzeti biztonsági stratégiájáról

[27] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

[28] 2151//2005. (VII. 27.) Korm. határozat a Terrorizmus Elleni Nemzeti Akcióterv felülvizsgálatáról

[29] 2046/2007. (III. 19.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól szóló 2112/2004. (V. 7.) Korm. határozat módosításáról

[30] 1249/2010. (XI. 19.) Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelvnek való megfelelés érdekében végrehajtandó kormányzati feladatokról

[31] 2003/2011. Korm. határozat az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelv végrehajtásáról és az Európai bizottság számára történő jelentésről

[32] 27/2004. (X. 6.) IHM rendelet az informatikai és elektronikus hírközlési, továbbá a postai ágazat ügyeleti rendszerének létrehozásáról, működtetéséről, hatásköréről, valamint a kijelölt szolgáltatók bejelentési és kapcsolattartási kötelezettségéről

[33] Az elektronikus közszolgáltatásról szóló 2009. évi LX. törvény (Ekszt.)

[34] A nemzeti adatvagyon körébe tartozó állami nyilvántartások védelméről szóló 2010. évi CLVII. törvény

[35] 38/2011. (III. 22.) Korm. rendelet a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozásának biztosításáról

[36] http://www.cert-hungary.hu Letöltés: 2011.11. 22.

[37] Kovács László: Kritikus infrastruktúrák Magyarországon. Robothadviselés 7. tudományos szakmai konferencia 2007. november 27. Hadmérnök Különszám http://www.hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html; (2011. 11. 22.)

[38] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai – Hadmérnök, 2008. (III.)/2., 138-148. o. http://www.hadmernok.hu/archivum/2008/2/2008_2_kovacsl.html; (2011. 11. 22.)

[39] Homeland Security Presidential Directive 7/HSPD-7, Washington, 2003. december 17. Idézi: Dr. Haig Zsolt - Hajnal Béla - Dr. Kovács László - Dr. Muha Lajos - Sík Zoltán Nándor: A kritikus információs infrastruktúrák meghatározásának módszertana. ENO Advisory Kft., 2009.

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Nagy Tibor István
nagy.tibor@nik.uni-obuda.hu

SZENZORHÁLÓZATOK SZOFTVERFEJLESZTÉSI KÉRDÉSEI

Absztrakt

A felügyelet nélküli szenzorhálózatok a civil szférában és a szárazföldi harcászati felderítésben egyaránt fontos szerepet játszanak. A legtöbb informatikai eszközhöz hasonlóan a szenzorok működéséhez a hardverösszetevőkön túl szoftverekre is szükség van, melyek a szenzorok vezérlését, a hálózat kiépítését, illetve a megbízható működést szabályozzák.
Ez a publikáció áttekintést ad a felügyelet nélküli rendszereknél leggyakrabban használt operációs rendszerekről, programozási nyelvekről, tervező- és fejlesztőeszközökről.

Unattended ground sensor networks are important in civil society and in ground reconnaissance. Like most of the devices in information technology, sensors also need hardware and software components to operate the sensors, build up the network between them and ensure reliable operation.
This paper gives a review of the operating systems, programming languages and development tools mostly used with unattended sensors.

Kulcsszavak: *szenzor, felügyelet nélküli szenzorhálózat, intelligens szenzorhálózat, tervezőeszközök, fejlesztőeszközök, IDE ~ sensor, unattended sensor network, intelligent sensor network, design tools, development tools, IDE*

1. BEVEZETŐ

A civil életben, a honvédelemben, rendvédelemben és a katasztrófavédelemben egyaránt találunk sok olyan tevékenységet, amelyeknek emberek általi végrehajtása nem megoldható, mert a célterület nem megközelíthető, túl nagy kockázattal jár, vagy nagypontosságú méréseket igényel. Ezen tevékenységek nagy részéből természetesen nem hagyható el az ember, de bizonyos részeit gépekre, elektronikára, mesterséges intelligenciára lehet – és célszerű is – bízni. Az emberi erőforrás nélkül megvalósítható tevékenységek közé általában az adatgyűjtés, különböző jellemzők mérése, vegyi- meteorológiai-, geológiai folyamatok megfigyelése tartoznak.

A lehetséges alkalmazási területek például az erdőtüzek megfigyelése, megfékezése, épületen belüli tűzvédelmi feladatok ellátása, árvizek, belvizek esetén adott terület geológiai, statikai jellemzőinek mérése, vulkáni tevékenység során lezajló folyamatok nyomon követése, harctéri ellenséges csapatmozgások, ellenséges erők megfigyelése, orvlövészek detektálása.

Az adatgyűjtést, jellemzők mérését szenzorok, érzékelők segítségével lehet elvégezni. Sokféle fizikai elven működő szenzor létezik, amelyek az általuk alkalmazott mechanizmus felhasználásával különféle fizikai paraméterek változásait képesek érzékelni. A szenzorok általában „egy csomagban” vannak az áramforrással, illetve vezérlő- és előfeldolgozó egységgel, amelyek a működésüket biztosítják. Ha nagy területet kell átfogni, figyelni, erre egyetlen ilyen csomag – más néven node – nem alkalmas az érzékelők korlátozott hatótávolsága, és energetikai paraméterei miatt, ezért legtöbbször ezekből többet kell a megfigyelt területen elhelyezni, amelyek egymással kapcsolatban állnak, és összehangoltan, egymás képességeit kiegészítve, a feladatokat egymás között megosztva működnek, azaz hálózatba szerveződnek. Az összehangolt működéshez a node-ok közti kommunikációra is szükség van, ezért a node-ok kapcsolattartást lehetővé tevő egységeket is tartalmaznak.

A szenzorhálózatok katonai alkalmazási területi, lehetőségei igen széleskörűek; leginkább az elektronikai felderítésben, és az elektronikai támogatásban bizonyulhatnak hatékony eszköznek, de kisebb változtatásokkal akár az elektronikai ellentevékenység terén is használhatóak.

Elsődleges felhasználási területként a harcászati felderítést lehet említeni, ahol az ellenséges csapatok mozgásával, létszámával, összetételével kapcsolatban lehet létfontosságú adatokat gyűjteni segítségükkel. Nagy előnyük, hogy nem kell a veszélyes területre felderítő katonákat küldeni és így értékes emberéleteket lehet megóvni, ami a további harcok sikerességét jelentősen befolyásolhatja.

A megfelelő vezérlés megvalósításához, a node-ok közti kapcsolat felépítéséhez és fenntartásához, a begyűjtött adatok átalakításához, továbbításához a hardverelemeken kívül természetesen szoftverekre is szükség van. Az optimális működéshez meg kell határozni a hardver- és szoftverösszetevők megfelelő arányát, a feldolgozást, átalakítást, adatfuzionálást ellátó szoftverelemek node-ok és bázisállomások közti megosztásának arányát, figyelembe kell venni a szoftverek futtatását lehetővé tevő operációs rendszer és a szoftverek elkészítéséhez használható tervező-, fejlesztő eszközöket, programozási paradigmákat, és programozási nyelvi sajátosságokat.

Ebben a cikkben a szenzorhálózatok szoftverfejlesztési kérdéseivel foglalkozom. Bemutatom a hálózatok tervezésének kérdéseit általában és a szenzorhálózati tervezés speciális feladatait. Végül csoportosítom a szenzorhálózatoknál használt szoftverelemeket, operációs rendszereket és fejlesztő eszközöket.

2. VEZETÉK NÉLKÜLI HÁLÓZATOK TERVEZÉSE

2.1. Hálózat fogalma [1]

Tanenbaum szerint a számítógépes hálózat olyan rendszer, amelyben a feladatokat „sok-sok különálló, de egymással összekapcsolt számítógép látja el”. [1]

Sokféle hálózati architektúra létezik, függően a felhasználás céljától, helyétől. A legegyszerűbb esetben két számítógép áll (közvetett vagy közvetlen) kapcsolatban egymással, és mindkét gép képes egymás szolgáltatásait igénybe venni (pont-pont kapcsolat). A két gép tekinthető egyenrangúnak, és mindkettőnél ül egy felhasználó, aki a saját, illetve a másik számítógépét használja (pl.: számítógépes játékok, bluetooth kapcsolat két gép között, stb.). A másik lehetőség szintén két gép közvetett, vagy közvetlen kapcsolata, de itt az egyik gép általában jóval nagyobb teljesítményű a másiknál. A kisebb teljesítményű gép használja a nagyobb teljesítményű szolgáltatásait (kliens-szerver architektúra).

Hálózatot természetesen nem csak számítógépek, hanem elektronikai eszközök (pl.: szenzorok) is alkothatnak, vagy akár vegyesen számítógépek és különböző elektronikai eszközök is. A rengeteg különböző igény, sokféle különböző eszköz miatt a hálózatok kizárólag elektronikai gyártással történő megvalósítása nem lehetséges. Emiatt megalkottak úgynevezett hálózati hivatkozási modelleket, amelyek különböző, egymástól elkülönülő rétegeket definiálnak, melyek egymástól függetlenül valósíthatóak meg, ezzel biztosítva az alkalmazási területek végtelen sorát.

Mindegyik modell lényege, hogy az egyes rétegek csak a közvetlenül alattuk, illetve felettük levő rétegekkel kommunikálhatnak meghatározott interfészeken keresztül. A rétegek fekete dobozként működnek, azaz elrejtik mások elől adataikat és működésük részleteit.

Minél magasabb szintű rétegről van szó, annál inkább tolódik el a működést biztosító technológia a hardver irányából a szoftver felé, illetve annál bonyolultabb, összetettebb funkciókat biztosít, és annál bonyolultabb, nagyobb adategységekkel képes dolgozni.

2.1.2. OSI hivatkozási modell:

A legrégibb, illetve legáltalánosabban használható modell. A többi modell általában ennek a specializált, konkrét igényekre átszabott változata. Hét réteget definiál:

- *Fizikai réteg:* Feladata a bitenkénti adattovábbítás megvalósítása az átviteli közeg felhasználásával. Ez a réteg az átvitel mechanikai, elektronikai kérdéseivel foglalkozik. A főszerepet itt a vezetékek, csatlakozók, áramkörök játsszák.
- *Adatkapcsolati réteg:* Az adatátviteli egység itt az adatkeret, amely néhány száz, vagy néhány ezer bájt. A réteg feladata a keretek helyes sorrendben és hibamentesen történő eljuttatása a küldőtől a fogadóig.
- *Hálózati réteg:* Feladata az adatcsomagok eljuttatása a küldőtől a fogadóig, illetve az ehhez használandó útvonal kiválasztása, csomagtorlódások megakadályozása, hálózati forgalom vezérlése. Ez a réteg általában a hálózati szolgáltatást nyújtó szolgáltató routerein működik. A legelterjedtebb protokollja az IP (Internet Protocol).
- *Szállítási réteg:* A viszonyrétegtől érkező információkat darabolja szét megfelelő méretű és szerkezetű adategységekké. A szállítási réteg hasonló funkciót biztosít mint a hálózati réteg, azzal a különbséggel, hogy általában a küldő, illetve a fogadó számítógépen működik. A szállítási rétegben leggyakrabban használt protokollok a TCP és az UDP.
- *Viszony réteg:* A réteg feladata két gép közötti viszony (session) létrehozása és kezelése. A viszonyban az adás jogának kiosztása, kritikus műveletek végrehajtási jogának szabályozása, kommunikáció szinkronizálása.

- *Megjelenítési réteg*: Bonyolultabb, illetve különböző típusú adatszerkezetek használatát és átvitelét teszi lehetővé.
- *Alkalmazási réteg:* A felhasználói programok által a hálózat lehetőségeinek használatához szükséges protokollokat tartalmazza. A leggyakrabban használt ezek közül a weblapok és egyéb webszervereken található erőforrások lekéréséhez használható http, de ide tartoznak az FTP a fájlok átviteléhez, elektronikus levelezés protokolljai (például az SMTP), stb.

2.1.3. TCP/IP hivatkozási modell:

Ez a hivatkozási modell az internet születésekor, annak hálózati modelljeként funkcionált, és a mai napig is ezt a szerepet tölti be. Több, különböző méretű, típusú, különböző technológiákat használó hálózat biztonságos, megbízható összekötését képes megteremteni és vezérelni.

- *Hoszt és hálózat közötti réteg:* A TCP/IP hivatkozási modellben ez a réteg nincs kidolgozva. Nem definiál semmilyen áramkört, átviteli közeget, fizikai kapcsolati módot, tehát a modell legalsó rétege tulajdonképp a következő internet réteg.
- *Internetréteg:* A TCP/IP hivatkozási modell központi rétege. Az elküldendő adatokat képes csomagokra felosztani és azt bármilyen típusú hálózatban található címzetthez eljuttatni. Protokollja az IP (Internet Protocol).
- *Szállítási réteg:* A réteg feladata az elküldendő adatok üzenetekké alakítása és az internetréteg felé történő továbbítása, és az adatátvitel sebességének szabályozása a küldő és fogadó sebességkülönbségétől függően. Protokollja a TCP (Transmission Control Protocol), amely az adatok biztonságos, és megfelelő sorrendű átvitelét biztosítja, illetve az UDP (User Datagram Protocol), amely nem nyújt biztonságos átviteli szolgáltatást, viszont gyors és kapcsolat nélküli módon valósítja meg az átvitelt.
- *Alkalmazási réteg:* Az OSI modell Megjelenítési- és viszonyrétege a TCP/IP modellben nincs külön rétegként definiálva. Ezek feladatait is az alkalmazási réteg látja el. Itt találhatóak azok a protokollok, amelyek a különböző felhasználói alkalmazások működéséhez szükségesek (FTP, HTTP, SMTP, TELNET, DNS, …).

2.2. Hálózattervezés főbb feladatai, célja, rendeltetése

Általánosságban nagyon tág a hálózattervezés fogalma. Az alsóbb rétegekben a hordozó média, topológiák tekintetében már kialakult rendszerek vannak, amelyeket a hálózattervezők használnak, és amelyet a hálózati eszközt gyártó cégek az eszközbe beépítve kínálnak (pl.: topológiák terén leginkább busz, illetve csillag topológiát alkalmaznak, UTP kábelt használnak a gépek és hálózati eszközök összekötéséhez, stb.).

Leginkább a futtatott szoftverek tekintetében lehet nagyobb feladatról beszélni, vagyis a felsőbb rétegek szoftvereinek megtervezése és elkészítése jelentik a hálózattervezők feladatának nagyobb kihívást jelentő részét, ide értve a meglévő protokollok használatát, vagy esetleg új protokollok kidolgozását is.

Általánosságban léteznek olyan hálózattervezési kérdések, amelyek egy hálózat működési paramétereit, minőségét meghatározzák. Ezeknek a rétegeknek a megvalósításával a hivatkozási modell egyes rétegei foglalkoznak.

Általános hálózattervezési kérdések [1]:

- Címzés: az üzenet fogadójának és küldőjének azonosítása;
- Hibavédelem: hibajavító kódok alkalmazása az átvitelnél okozott adatvesztés, vagy hibák kijavítására, üzenetek megfelelő sorrendjének biztosítása;
- Forgalomszabályozás: a különböző sebességű adók és vevők szinkronizálása;

- Multiplexelés: egy csatornán több kommunikáló számítógéppár üzenetei összefésülve kerülnek átküldésre;
- Forgalomirányítás: annak meghatározása, hogy az adatok milyen útvonalon jussanak el a feladótól a címzettig, hogy a leggyorsabban, legkisebb hálózati terheléssel, legbiztonságosabban érkezzenek meg.

2.3. Szenzorhálózatok hálózattervezésének sajátos feladatai

A szenzorhálózatok esetén is az OSI modell rétegei, illetve ezek összevonásából kialakult új rétegek használatosak az egyes feladatok különböző szinten történő megvalósítására. A specialitást itt az adja, hogy a node-ok esetében figyelembe kell venni néhány olyan jellemzőt, amelyek a hagyományos számítógép-hálózatoknál nem okoznak problémát. Ilyen például a szűkösen rendelkezésre álló energia, a node-ok esetleges helyváltoztatásának, illetve működésképtelenségének problémája, illetve a feladatok egyes node-ok közti elosztásának módja. Ezekre a specialitásokra alkották meg a WSN protokoll-vermet.

WSN (Wireless Sensor Network) protokoll-verem [2]:

Egy kockaként ábrázolható, amely síkokra, illetve rájuk merőleges rétegekre van osztva. A síkok a szenzorhálózat működésének legkritikusabb, egymástól elkülönülő feladatcsoportjait jelenítik meg, amelyek esetén az egyes rétegeknél más és más tervezési szempontokat kell figyelembe venni. Ezek a síkok biztosítják azt is, hogy az egyes rétegek ne csak a közvetlenül alattuk lévő rétegekkel tudjanak kommunikálni, hanem a többi réteg által előállított, de az aktuális réteg által igényelt adatokkal is tudjanak dolgozni. Ez az OSI modell eredeti szándékát – miszerint a rétegek jól elszeparált egységek, melyek működésüket elrejtik a külvilág elől, és csak a közvetlenül alattuk, illetve fölöttük lévő rétegekkel kommunikálhatnak – nem veszi figyelembe, de könnyebbé teszi a konkrét szenzorhálózati megvalósítások elkészítését. Többféle protokoll-vermet is definiáltak, ezek közül itt kettőt írok le: az egyik három, míg a másik négy síkot definiál.

Három síkot definiáló változat:

- Energia-menedzsment sík: Itt a legfontosabb figyelembe veendő szempont, hogy az egyes node-ok minél kevesebb energia felhasználásával tudják ellátni feladatukat, ezzel minél hosszabb ideig legyenek képesek működni. Ez biztosítható minél jobb akkumulátorok használatával, olyan kiegészítő eszközökkel, amelyek a környezetből képesek energiát felvenni, illetve az egyes node-ok közötti feladatok elosztásával az akkumulátorok töltöttségi szintjeitől függően.
- Mobilitás-menedzsment sík: léteznek olyan szenzorhálózatok, melyekben az egyes node-ok képesek a telepítést követően változtatni helyzetüket, esetleg néhány közülük elromolhat, szándékos rongálás következtében elpusztulhat. A telepítés jellegétől függően közvetlenül a telepítés után szükség lehet a node-ok helyzetének felderítésére, hogy a hálózati kapcsolatot ki lehessen közöttük építeni, ami szintén ennek a síknak a feladata.
- Feladat-menedzsment sík: a feladatok kiosztása, adattovábbítás, adatfeldolgozás, tömörítés, kódolás, feladatok párhuzamosítása, illetve elosztott feladat-végrehajtás tartoznak ennek a síknak a feladatkörébe.
- Négy síkot definiáló változat [3]:
- Energia-menedzsment sík: megegyezik a három síkot definiáló változatnál ismertetettel.
- Biztonsági sík: az adatok titkosítása, kódolás, dekódolás a feladata.
- Időszinkronizációs sík: az egyes node-ok időbeli összehangolása tartozik a feladatkörébe.

- Szomszédfelderítő sík: egy node szomszédjainak felderítését, a szomszédok megkeresését, lekérdezését teszi lehetővé.

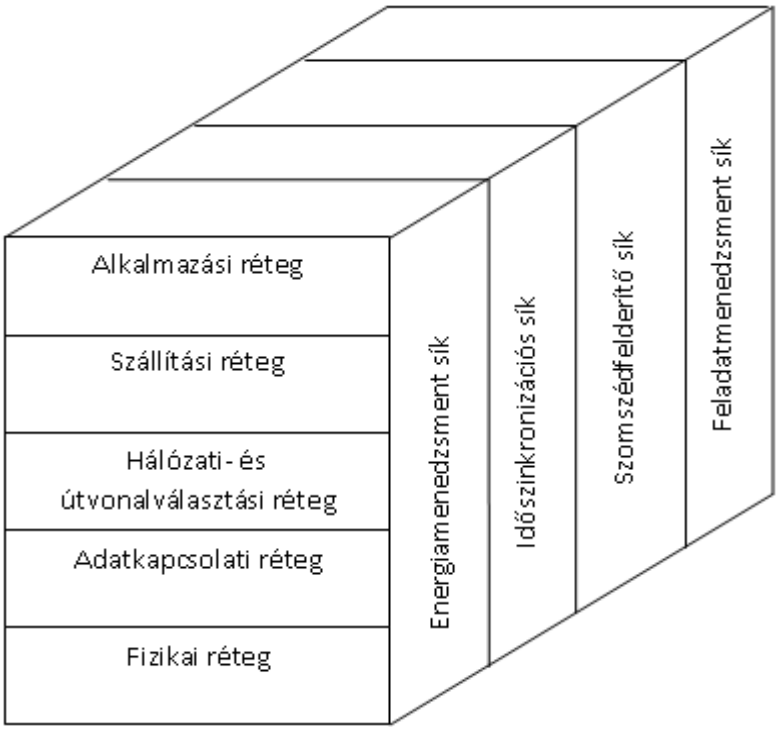
A második protokoll-verem még ezen kívül egy negyedik dimenziót is bevezet, amely szétválasztja egymástól az adatok kezelését és a vezérlést a különböző síkok és rétegek metszeteiben.

A rétegek pedig:

- Fizikai réteg: ez a réteg a kommunikáció fizikai paramétereivel foglalkozik, mint a frekvencia kiválasztása, modulációs mód, jelfelismerés, jelátalakítás, kódolás. Ezek a jellemzők leginkább a hardver szintjén megvalósíthatók.
- Adatkapcsolati (MAC) réteg: a hálózat kiépítését végzi, meghatározza a hálózati topológiát, az üzenetküldés módját, biztosítja a megbízható hálózati kapcsolatot, illetve az átküldött adatokban keletkezett hibák kijavítását.
- Hálózati és útvonal-választási réteg: legfőbb feladata az útvonalválasztás, ahol is az egyes node-ok megcímzése attribútum központúan történik, az optimális energiafelhasználás, illetve a lehető legjobb jelerősség biztosítása mellett.
- Szállítási réteg: feladata a különböző típusú hálózatok összekötése lenne. Erre a feladatra a TCP / UDP protokollok a legmegfelelőbbek, ezeknek, vagy ezeknek a speciális igényekhez igazított változatai használhatóak.
- Alkalmazási réteg: a réteg feladatai nagyrészt hasonlóak az OSI modellnél ismertetettekkel. Az itt alkalmazható protokollok fejlesztés alatt állnak, több kutatási projekt is foglalkozik ezzel a kérdéssel. Az egyik ilyen protokoll az SMP (Sensor Management Protocol), amely a szenzorok adminisztrátorok általi, távoli (például internetes kapcsolaton keresztüli) vezérlését teszik lehetővé. A másik a TADAP (Task Assignment and Advertisement Protocol), amely a felhasználók számára érdekes adatok, illetve node-ok kiválasztását teszik lehetővé, a harmadik pedig az SQDDP (Sensor Query and Data Dissemination Protocol), melynek segítségével lekérdezések formájában lehet hozzájutni a kívánt adatokhoz az SQLT (Sensor Query and Tasking Language) segítségével.

Felmerülhet a kérdés, hogy a protokoll-verem megvalósítások közül melyik lenne a legjobb a katonai alkalmazások esetén – különös tekintettel a kutatási témára: az ad hoc szervezésű, szárazföldi harcászati szenzorhálózatokra –, vagy lehetne-e a két változat ötvözetét használni. Véleményem szerint a síkok uniója nem lenne megfelelő modell, hiszen hat különböző sík, plusz még az adatok és a vezérlés szétválasztása átláthatatlanná és nehézkessé tenné a tervezést. A biztonságos adattovábbításnak fontos szerep jut, de szerintem nincs szükség rá, hogy több réteg is foglalkozzon ezzel a kérdéssel. A mobilitás-menedzsment csak olyan hálózatoknál fontos, ahol a node-ok helyet tudnak változtatni. A szinkronizáció az összadatforrású felderítés miatt lényeges, hiszen egy célpont észleléséhez szükséges a különböző típusú szenzoroktól érkező adatokról pontosan tudni, hogy mikor mérték őket. A repülőgépről történő kiszórással, vagy tüzérségi eszközzel történő telepítés esetén ad hoc hálózat alakul ki, melyben a szomszédok felderítésének nagy a jelentősége. Az energia-menedzsment természetesen nem elhagyható, fontos szempont, ezért ennek a síknak a megtartása is lényeges lehet. A feladatok szétosztása szintén olyan tevékenység, melyről több réteg is kell, hogy tudjon, hiszen például az alkalmazás réteg csak akkor tudja a megfelelő node-oknak továbbítani a kiválasztott feladatrészt, ha tudja, hogy mely node-ok képesek a működőek közül végrehajtani azt.

Ez alapján az általam javasolt WSN protokoll-verem az 1. ábrán látható.



1. ábra. Javasolt WSN protokoll verem

3. SZOFTVERTERVEZÉS SZENZORHÁLÓZATOKBAN

3.1. Szoftverfejlesztés szerepe szenzorhálózatokban

A node-ok érzékelőket, kommunikációs részegységeket, memóriát és az ezek vezérlését végző processzort tartalmaznak, vagyis a node-ok speciális számítógépek. Mint ilyenek, természetesen nemcsak hardvert, hanem szoftvert is tartalmaznak. Bizonyos funkciók előre huzalozottan, a gyártó által beépítve állnak rendelkezésre, más funkciókat pedig szoftverek segítségével kell megvalósítani. Az alacsonyabb szintű szoftveres funkciókat operációs rendszerek biztosítják, míg a magasabb szintű, bonyolultabb, összetettebb feladatokat az operációs rendszer által futtatható programok látják el.

A szoftver- és hardverelemeknek három fő feladatcsoportot kell ellátniuk:

- Információszerzés: adatok begyűjtése a szenzoroktól;
- Adatfeldolgozás: a szenzoroktól begyűjtött adatok továbbítható formára alakítása, megfelelő adatszerkezetekbe foglalása, a mért jellemzők jellegének és a mérés idejének rögzítése, hibajavító kódok alkalmazása, adatok titkosítása;
- Adattovábbítás: a begyűjtött és előfeldolgozott adatok továbbítása egy gyűjtőcsomóponthoz, meghatározott útvonalon, figyelembe véve az optimális energiafelhasználást.

3.2. Operációs rendszerek

Az operációs rendszerek biztosítják a programok futtatását és a hardver programból történő elérésének lehetőségét. A node-okon többféle operációs rendszer is használható, amelyet a következőkben sorolok fel:

- *Contiki:* nyílt forrású, eseményvezérelt, többfolyamatos és egyszerűsített szálkezeléses operációs rendszer, amely hálózatba kötött beágyazott rendszereken és szenzorhálózatokon működik. Tipikusan 2 kbyte RAM-ot és 40 kbyte ROM-ot igényel, vagyis kevés memóriával rendelkező eszközökön képes működni. IPv4 és IPv6 kommunikációt biztosít alacsony energiafelvétel és szoftveres

energiamenedzsment mellett. A TCP/IP hivatkozási modell egyes rétegeiben saját fejlesztésű protokollokat alkalmaz. Saját fájlrendszert használ a node-okon történő adattároláshoz. A szoftverfejlesztés C nyelven történik, a kész szoftverek tesztelésére pedig szimulátorok állnak rendelkezésre. [4]

- *LiteOS:* dinamikus memóriakezelésű, többszálas programokat futtatni képes operációs rendszer, amely UNIX-szerű hierarchikus fájlrendszert használ. Lehetővé teszi az alkalmazások telepítés utáni frissítését / újratelepítését. A node-okhoz terminálparancsok segítségével lehet hozzáférni. A programok fejlesztése C nyelven történik, az AVR Studio fejlesztőkörnyezet pedig megkönnyíti a programozó munkáját. Különlegessége, hogy minden protokoll egy-egy szálként van megvalósítva, így a beépített protokollok könnyen lecserélhetők sajátra, vagy akár több protokoll is megfér egymás mellett. [5]
- *NanoQplus:* nyílt forrású, szálkezelés-központú operációs rendszer. A szálak ütemezése preemptív „round-robin" módszerrel történik. A memóriatakarékosságot egy speciális lapozó technikával valósítja meg, amely a működés sebességének a csökkenésével járhat. Kernel szinten tartalmaz olyan funkciókat, amelyek az útvonalválasztást, node-ok felderítését valósítják meg. Léteznek hozzá grafikus fejlesztőeszközök az automatikus kódgeneráláshoz, távoli monitorozáshoz, illetve távoli szoftverfrissítéshez. [6]
- *TinyOS:* nyílt forrású, komponensalapú, eseményvezérelt operációs rendszer. Nem támogatja a dinamikus programfuttatást / telepítést, programok frissítését és a dinamikus memóriakezelést. A programok nesC nyelven íródnak, komponensekből tevődnek össze, amelyek egymáshoz interfészeken keresztül kapcsolódnak. A végrehajtási modellje nem blokkoló, azaz a hosszabb időt igénybe vevő feladatok aszinkron hajtódnak végre. Egyszerű folyamatkezeléssel rendelkezik. Az eseményvezérelt, aszinkron működés és az egyszerű folyamatkezelés miatt az összetettebb feladatokra programot készíteni nehézkes. A szenzorhálózatoknál ez a legelterjedtebb operációs rendszer, ezért sokféle node-ot támogat. [7]

Ezen operációs rendszerek mindegyike megvalósítja a hálózati hivatkozási modell rétegeit vagy már létező, vagy saját protokollok segítségével.

A felsoroltakon kívül még sok szenzorhálózatoknál használható (Erika Enterprise, SOS, Nano-RK, …), illetve általános beágyazott rendszereken működő (Windows CE, embedded Linux, VxWorks, eCos, SymbOS, …) operációs rendszer létezik, de a fentiek a legelterjedtebbek és paramétereiket tekintve leginkább illeszkednek a szenzorhálózatok által támasztott igényekhez.

A megfelelő operációs rendszer kiválasztásánál több szempontot is érdemes figyelembe venni: a kiszemelt node típust támogatja-e, mennyire kényelmes a fejlesztés (fejlesztőeszközök, fejlesztőkörnyezetek), mennyi RAM, ROM, flash memória szükséges a működéséhez, illetve az elkészített programok frissíthetőek-e. Az első szempontnak a TinyOS felel meg a leginkább, hiszen ez a legrégebben használt, legelterjedtebb operációs rendszer, viszont a komponens alapú, eseményvezérelt működés és a túl egyszerű folyamatkezelés miatt nem biztosít kényelmes és nem rugalmas szoftverfejlesztést. A felsoroltak közül mindegyik kimondottan kevés erőforrással rendelkező eszközökre lett optimalizálva, ezért nincs nagy eltérés közöttük a memóriahasználat tekintetében. Az elkészített programok frissíthetőségét a Contiki és a LiteOS lehetővé teszi, ezen kívül mindkettőhöz létezik kényelmesen használható fejlesztőeszköz, illetve szimulátorok a tesztelés megkönnyítésére. A fejlesztőeszközök tekintetében a TinyOS sem marad le, hiszen az Eclipse-hez telepíthetőek kiegészítők, melyekkel TinyOS-re lehet programot fejleszteni, illetve a NanoQplus-hoz is léteznek fejlesztő, telepítő és monitorozó eszközök. A fentiek alapján véleményem szerint a legjobb operációs rendszerek a felsoroltak közül a Contiki és a LiteOS.

3.3. Információszerző szoftverelemek

A szenzorok működtetésének alapfunkcióit huzalozottan valósítják meg. A szenzoroktól érkező adatok elérését, az energiamenedzsment funkciókat az operációs rendszerbe építik be. Az egyes operációs rendszerek más és más módon valósítják meg ezeket, és a felhasználói alkalmazások ezeket rendszerhívásokon keresztül érhetik el. Az operációs rendszerek többsége biztosít lehetőséget a beépítetten megvalósított módszer sajátra történő lecserélésére.

3.4. Adattovábbító szoftverelemek

Huzalozottan csak a rádió adóvevő működtetését készítik el, az útvonalválasztást, adatok eljuttatását egyik node-tól a másikig, egy adott node-tól a gyűjtő csomópontig (sink node) az operációs rendszer valósítja meg egy meghatározott protokoll szerint, amely operációs rendszerenként különböző lehet. Az operációs rendszerek többsége biztosít lehetőséget a beépítetten megvalósított módszer sajátra történő lecserélésére.

3.5. Adatfeldolgozó szoftverelemek

A szenzortól érkező adatok előfeldolgozásához (konverzió, tömörítés, titkosítás, megfelelő struktúrába szervezés, …) sem huzalozott, sem operációs rendszerbe beépített megoldások nem léteznek. Erre szoftvert kell készíteni. Operációsrendszer-szinten az adatok tárolásának lehetősége biztosított valamilyen egyedi fájlrendszer-megoldással, vagy például a Contiki operációs rendszerben egy node-okon használható adatbáziskezelő rendszerrel.

A bázisállomásokon történő adatfeldolgozáshoz, adattároláshoz egyrészt használhatóak a kereskedelmi forgalomban kapható általános célú adatbáziskezelő rendszerek egy megfelelő szoftver-kiegészítéssel, amely összekapcsolja ezt a rendszert a szenzorhálózattal. Képfeldolgozáshoz, képfelismeréshez, adatfúzióhoz saját szoftvert kell készíteni.

Az adatok megjelenítéséhez, vizualizálásához a legtöbb operációs rendszer tartalmaz távoli parancssori elérési lehetőséget, amellyel a node-ok, illetve szenzoraik állapotai és az általuk szolgáltatott adatok lekérdezhetők. Ezen kívül van olyan operációs rendszer, amely grafikus felhasználói felülettel rendelkező alkalmazást is rendelkezésre bocsájt ugyanezen feladat ellátására.

4. KONKLÚZIÓ

A szenzorhálózatok az élet legkülönbözőbb területein felhasználhatóak az ipari gyártástól az intelligens otthon vezérlésén keresztül a harctéri felderítési feladatok ellátásáig. A hagyományos számítógépekhez, illetve ezeket összekötő hálózatokhoz hasonlóan itt is szükség van szoftverekre a megfelelő működés biztosításához, illetve a rugalmas, skálázható, bővíthető rendszer kialakításához. Ez a cikk áttekintést adott a hálózatok tervezésének általános, és szenzorhálózatoknál alkalmazandó technikáiról, tervezési elveiről, módszereiről, és a különböző feladatcsoportok esetén rendelkezésre álló szoftverelemekről.

Felhasznált irodalom

[1] A. S. TanenBaum: Számítógép-hálózatok, Második, bővített kiadás, Panem Könyvkiadó Kft., 2004. ISBN 963 545 384 1

[2] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci: Wireless sensor networks: a survey, Computer Networks 38, 2002, pp 393-422. http://www.larces.uece.br/~celestino/RSSF%20I/Wireless%20Sensor%20Networks%20a%20Survey.pdf; (letöltés: 2012. 01. 30.)

[3] Siddhart Ramesh: A Protocol Achitecture for Wireless Sensor Networks, University of Utah. http://www.cs.utah.edu/~sramesh/attachments/sensornet_archi.pdf; (letöltés: 2012. 01. 30.)

[4] A Contiki OS hivatalos weboldala, http://www.contiki-os.org/; (letöltés: 2012. 02. 24.)

[5] Q. Cao, T. Abdelzaher, J. Stankovic, T. He, The LiteOS Operating System: Towards Unix-like Abstractions for Wireless Sensor Networks, IPSN '08: Proceedings of the 7th international conference on Information processing in sensor networks, pp 233-244. IEEE Computer Society, 2008.

[6] S.C. Kim, H. Kim, J.K. Song, M. Yu, P. Mah: NanoQplus : A Multi-Threaded Operating System with Memory Protection Mechanism for WSNs, Proceedings of the CKWSN, 2008, http://nano-os.tistory.com/attachment/cfile23.uf@135FD6484DC6900E2BC27E.pdf; (letöltés: 2012. 02. 26.)

[7] P. Levis: TinyOS 2.0 Overview, 2006, http://wiesel.ece.utah.edu/redmine/projects/wasp/repository/revisions/f4407f25ded5a962bd0ed34c950b49f29a88a4a3/raw/doc/pdf/overview.pdf; (letöltés: 2012. 02. 26.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Nagy Tibor István
nagy.tibor@nik.uni-obuda.hu

SZENZORHÁLÓZATOKKAL SZEMBEN TÁMASZTOTT TEREPI KÖVETELMÉNYEK

Absztrakt

A felügyelet nélküli szenzorhálózatok a civil szférában és a szárazföldi harcászati felderítésben egyaránt fontos szerepet játszanak. A legtöbb informatikai eszközhöz hasonlóan a szenzorok működéséhez is szükségesek a hardverösszetevők, melyeknek jellemzői jelentős mértékben befolyásolják a felhasználás módját és helyét.
A szárazföldi harcászati felderítésben a terep meteorológiai, geológiai körülményei speciális követelményeket támasztanak a szenzorokkal, node-okkal és az ezekből felépülő hálózatokkal szemben.
Ez a publikáció áttekintést ad a felügyelet nélküli rendszereknél releváns terepi követelményekről, a létező implementációkról és ezek jellemzőiről.

Unattended ground sensor networks are important in civil society and in ground reconnaissance. Like most of the devices in information technology, sensors also need hardware components. The parameters of these components significantly modify the location and mode of usage.
In ground surveillance, the meteorological, geological characteristics of the target field implies special requirements for sensors, nodes and the networks made up by these components.
This paper gives a review of the relevant field requirements sensor networks need to fulfill, and of the implementations of these requirements and their characteristics.

Kulcsszavak: *szenzor, felügyelet nélküli szenzorhálózat, intelligens szenzorhálózat, terepi követelmények ~ sensor, unattended sensor network, intelligent sensor network, field requirements*

1. BEVEZETŐ

Az adatgyűjtést, jellemzők mérését szenzorok, érzékelők segítségével lehet elvégezni. Sokféle fizikai elven működő szenzor létezik, amelyek az általuk alkalmazott mechanizmus felhasználásával különféle fizikai paraméterek változásait képesek érzékelni. A szenzorok általában „egy csomagban" vannak az áramforrással, illetve vezérlő- és előfeldolgozó egységgel, amelyek a működésüket biztosítják. Ha nagy területet kell átfogni, figyelni, erre egyetlen ilyen csomag – más néven node – nem alkalmas az érzékelők korlátozott hatótávolsága, és energetikai paraméterei miatt, ezért legtöbbször ezekből többet kell a megfigyelt területen elhelyezni, amelyek egymással kapcsolatban állnak, és összehangoltan, egymás képességeit kiegészítve, a feladatokat egymás között megosztva működnek, azaz hálózatba szerveződnek.

A terepi követelmények meghatározzák, hogy a célterületen alkalmazandó eszközök milyen paraméterekkel kell, hogy rendelkezzenek annak érdekében, hogy a környezeti hatásoknak képesek legyenek ellenállni, és képesek legyenek megfelelő pontossággal, gyorsasággal végrehajtani a rájuk bízott feladatot. A szenzorhálózatoknál – és különösen harctéri alkalmazásuk esetén – a terepi követelményeknek való megfelelésnek korlátokat szabnak a méretek, az ellenség általi felfedezhetőség csökkentési igénye, a hardverelemek energetikai paraméterei, fogyasztása, és még sok más szempont ezen túlmenően is.

Ebben a cikkben a szenzorhálózatokkal kapcsolatos terepi követelményeket mutatom be. A szenzorhálózatok alapjaival kezdem, ezen belül a szenzorok fogalmát, típusait, működési jellemzőiket, paramétereiket foglalom össze, illetve csoportosítom a szenzorhálózatokat. Majd bemutatom az általános, és a szenzorhálózatokra vonatkozó terepi követelményeket és végül elemzem a terepi követelmények megvalósításait.

2. SZENZORHÁLÓZATOK ALAPJAI

Szenzorhálózat definíciója: 1.„Szenzorhálózatnak nevezzük nagyszámú, független (autonóm) intelligens érzékelőkből alkotott kooperatív hálózatot, ahol az egyes érzékelők valamilyen közös feladat végrehajtását elosztott módon valósítják meg." [1] Tehát a szenzorhálózatban autonóm működésű eszközök találhatóak, vagyis telepítésük után külső beavatkozás nélkül képesek ellátni feladatukat. Ehhez nyilván szükséges, hogy az eszköz rendelkezzen valamilyen vezérlőegységgel, amely a részegységeket irányítja, és megbízható, hosszú élettartamú energiaforrásra, amely a lehető leghosszabb ideig képes a részegységek működéséhez szükséges energiát biztosítani. Ezen kívül szükség van huzalozott, vagy tárolt formában szoftverre is, amely képes a vezérlőegység és a részegységek működését módosítani a működési feltételek megváltozása esetén, illetve amely a mért adatok előfeldolgozását, átalakítását el tudja végezni. Ilyen autonóm eszközökből a szenzorhálózatban több is működik; ezek egymással kommunikálnak, adatot cserélnek, reagálnak a többi eszköz állapotváltozásaira. A számítógépes hálózatokban ismert elosztott működéssel ellentétben itt nem a számítási kapacitás növelése a cél, hanem nagyobb terület lefedése, azaz egy eszköz által biztosított korlátozott hatótávolság kiterjesztése. Az eszközök egymással való kommunikációja történhet vezetékes, illetve vezeték nélküli kapcsolaton keresztül is. Az olyan feladatokhoz, melyeknél nem akadályozó tényező a vezetékek elhelyezkedése, illetve ahol a vezeték nélküli kapcsolat nem használható (pl.: rádiófrekvenciás zavarok miatt), ott a vezetékes megoldást alkalmazzák: például ipari gyártási folyamatokban, épületek fűtésének, világításának vezérlésénél.

UGS (Unattended Ground Sensors) definíciója: Nyílt terepre telepítik, autonóm a működése, akkumulátorról működik, rádióhullámok segítésével teremt vezeték nélküli kapcsolatot. [2] A felügyelet nélküli Szenzorhálózat elnevezést általában a haditechnikában,

azon belül is a harcászati felderítésben használatos fogalom. Tulajdonképpen ugyanazok a jellemzői, mint a szenzorhálózatoknak általában, kivéve hogy felhasználási helyéből adódóan néhány speciális követelménynek kell elege tennie. Ez is node-okból tevődik össze, amelyek egymással rádióhullámok segítségével kommunikálnak, speciális burkolattal rendelkeznek annak érdekében, hogy környezeti, vagy ellenséges rongálással szemben ellenállóak legyenek, vagyis speciális terepi követelményeknek kell eleget tenniük.

2.1. Szenzorok

A Node-ok a szenzorhálózatok önálló működésre képes egységei, amelyek szenzorokat tartalmaznak a különböző környezeti jellemzők mérésére, kommunikációs részegységet a többi node-dal való kapcsolattartásra, illetve akkumulátort a működéshez szükséges energia biztosítására. Egy node általában egy-, vagy többfajta szenzort tartalmazhat. Ezek működési mechanizmusuktól függően más és más környezeti jellemző érzékelésére képesek.

A szenzorok működtetéséhez, a mérési folyamat levezényléséhez, a környezetből vett jelek átalakításához, a működéshez szükséges energia biztosításához természetesen szükség van valamilyen elektronikára, amelyet az ún. node-ok, vagy másnéven mote-ok tartalmaznak (az érzékelőkkel együtt).

2.1.2. Szenzorok típusai: [2]

- Jelérzékelési mechanizmus alapján:
  - Passzív: a természetes energiamező célpont általi változásait érzékeli. Ezek az érzékelők tehát egy célpont által kibocsájtott jel érzékelésére alkalmasak, mint például egy jármű motorjának a hangja, a motor által felmelegedett burkolat hőkibocsájtása, stb.
  - Aktív: valamilyen energiahullámot bocsájt ki, melynek célpontról történő visszaverődését képes érzékelni. Erre példa a radar, amely a kibocsájtott rádióhullámok visszaverődése alapján érzékeli a járműveket.
- Mért jellemzők alapján:
  - Akusztikus [3]: A hanghullámokat érzékeli. Passzív változatai a célpont által előidézett légnyomásváltozásokat, míg aktív változatai a kibocsájtott ultrahangok célpontról történő visszaverődését detektálják.
  - Szeizmikus: mechanikai rezgések érzékelésére képes. Eltérő lehet az érzékelt rezgés frekvenciája, amplitúdója, és ez alapján többféle felhasználási területe is létezik a haladó járművek észlelésétől a vulkánok szeizmikus aktivitásának méréséig.
  - Mágneses [4]: A mágneses tér változását méri.
  - Elektro-optikai képi: az ilyen érzékelő a tárgyak, élőlények megjelenését, eltűnését képes érzékelni. Megfelelő szoftveres módosítással a képi információk továbbítására, azokon alakzatok felismerésére is felkészíthető.
  - Infravörös képi: a megfigyelt területen található tárgyak, élőlények által kibocsájtott hőt képes érzékelni, és ebből egy képet tud előállítani, amelyen a magasabb hőmérsékletű területek élénkebb, világosabb színnel, míg az alacsonyabb hőmérsékletűek sötétebb színnel jelenek meg.
  - Nyomás: a környezet nyomásváltozását (légnyomás, víz alatti nyomásváltozás) képes érzékelni.
  - Rádiófrekvenciás rezgés: rádióhullámokat képes érzékelni.
  - Kémiai / biológiai / nukleáris: a megfigyelt célterületen egy bizonyos kémiai, biológiai anyag koncentrációját, illetve sugárzó anyag sugárzási értékeit képes érzékelni.

- Mechanikai és infravörös: bizonyos mechanikai jellemzők (pl.: súrlódás), illetve a hőmérséklet megváltozását képes érzékelni.
- Meteorológiai: légnyomás, relatív páratartalom, hőmérséklet érzékelésére képes.

Az 1. táblázatban egy összefoglalás található a szenzorok típusai különböző szempont szerinti csoportosításának összefüggéseiről.

	Aktív	Passzív
Akusztikus	✓	✓
Szeizmikus		✓
Mágneses		✓
Elektro-optikai képi		✓
Infravörös képi		✓
Nyomás		✓
Rádiófrekvenciás rezgés	✓	✓
Kémiai/biológiai/nukleáris		✓
Mechanikai és infravörös	✓	✓
Meteorológiai		✓

1. táblázat. Szenzortípusok jelérzékelési mechanizmusa

2.1.3. Szenzorok jellemzői:

A szenzorokat jellemzi hatótávolságuk, pontosságuk, működési élettartamuk, fogyasztásuk és áruk.

Különböző publikációkban különböző jellemzőket tulajdonítanak az egyes szenzorfajtáknak. Véleményem szerint általánosságban nehéz ezeket összehasonlítani egymással, mivel minden szenzortípuson belül vannak érzékenyebb és kevésbé érzékeny, pontosabb, kevésbé pontos változatok, stb. Ami objektíven elmondható minden szenzor esetén, az az egyes jellemzők közti összefüggés, amelyet a 2. táblázat ábrázol. Természetesen ezek az összefüggések sem mindig teljesen egyértelműek (például az ár egy olyan jellemző, amelyet egyéb tényezők is befolyásolnak, mint például az, hogy ki gyártja a szenzort, mennyiért tudja beszerezni az alapanyagot, milyen a gyártó ország gazdasági környezete, stb).

	Hatótávolság	Pontosság	Élettartam	Fogyasztás	Ár
Hatótávolság		**fordított**	**fordított**	**egyenes**	**egyenes**
Pontosság			**fordított**	**egyenes**	**egyenes**
Élettartam				**fordított**	**egyenes**
Fogyasztás					**fordított**
Ár					

2. táblázat. Szenzorjellemzők viszonya

2.2. Szenzorhálózatok

A szenzorhálózatok különböző szenzorok és az őket működtető egységek hálózatba szervezett működését biztosító infrastruktúrát jelentik, melyben az egyes csomópontok (node-ok, mote-ok) egymással kapcsolatot tudnak teremteni és megosztottan adatfeldolgozási, illetve adattovábbítási feladatokat tudnak végrehajtani. A hálózatba szerveződés előnye az önálló feladatvégzéshez képest a feladatok szétosztásának, egy adott feladat elosztott megvalósításának, illetve a nagyobb hatótávolság elérésének lehetősége.

Nagyobb hatótávolság:

- Az érzékelés hatótávolsága egy szenzor esetén korlátozott. A hatótávolságot a szenzor jelérzékelési mechanizmusa, a mérési mechanizmus és a szenzor fogyasztása is befolyásolja. Több szenzor telepítése nagyobb területre képes kiterjeszteni az érzékelési mezőt.
- Az érzékelt adatok továbbításának is megvannak a távolsági korlátai. Elvárás a node-októl, hogy minél kisebb legyen az energia-felvételük a minél hosszabb élettartam, és – katonai alkalmazások esetén – a minél nehezebb ellenség általi felderíthetőség miatt. Az alacsony fogyasztású rádióadó azonban kisebb hatótávolságot képes csak biztosítani, ezért a mért adatok továbbításához több node közbeiktatására van szükség.

Szenzorhálózat elemei:

- Adatgyűjtő állomás: ez lehet egy épületben, vagy járművön elhelyezett adatgyűjtő központ, amely a csomópontok által mért jellemzőket tudja összegyűjteni.
- Node:
  - csak érzékelő: egy olyan csomópont, amelynek mindössze a környezeti jellemzők mérése, és a mért adatok továbbítása a feladata;
  - adatelosztó- vagy kommunikációs központ: kialakítástól függően a hálózatban lehetnek olyan csomópontok, amelyeknek elsődleges feladata az adatforgalom irányítása, adatok továbbítása, vett jelek felerősítése.

Ad hoc hálózatok

Adhoc hálózatok definíciója Buttyán, Holczer, Schaffer szerint: „ad hoc hálózat az, melyben a résztvevők előre telepített hálózati infrastruktúra igénybevétele nélkül, önszervező módon hozzák létre és működtetik a hálózatot. Infrastruktúra hiányában az alapvető hálózati funkciókat maguk a résztvevők látják el.” [5]

A definíció legfontosabb eleme, hogy nincs hálózati infrastruktúra, vagyis nincsen előre meghatározva az egyes csomópontok helye, funkciója és kapcsolatai a többi csomóponttal. Emiatt a csomópontoknak kell maguktól megkeresni a többi csomópontot és kialakítani a kapcsolatot egymás között. A harctéri szenzorok esetében a node-ok telepítési módjából adódhat az ad hoc hálózati kialakítás. A telepítés történhet tüzérlövegek segítségével, vagy repülőgépről kiszórással. Egyik változatnál sem biztosítható a pontos elhelyezés, illetve a biztonságos, sérülésmentes megérkezés sem, így aztán a telepítés után lehet csak a hálózat kialakítását elvégezni, a csomópontok pontos funkcióit kiosztani, amihez emberi erőforrás nem áll rendelkezésre, tehát a csomópontoknak maguknak kell ezt a feladatot is ellátni.

3. TEREPI KÖVETELMÉNYEK RENDSZERE

3.1. Általános terepi követelmények [6]

„A speciális terepi kivitelű informatikai eszközök az általánosan használatos informatikai eszközökkel szemben nem irodai, hanem keményebb környezeti feltételek közötti – üzemi, szabadtéri (terepi), vagy járművön történő (menet közbeni) – alkalmazás céljára tervezett készülékek.” [6]

Speciális követelmények a következők lehetnek:

- emberi tényezők elleni védelem: védelmet kell biztosítani a leejtés, kiömlő folyadék, és hasonló, emberi figyelmetlenségből, ügyetlenségből adódó problémák kiküszöbölésére;
- környezeti hatások elleni védelem: az eszköz működési környezetében előforduló külső – általában meteorológiai – hatások által okozható károk kiküszöbölése. Ide tartozik a magas páratartalom, túl magas, vagy túl alacsony hőmérséklet, a levegő magas porkoncentrációja, köd, eső, szél, stb;

– elektromágneses zavarok elleni védelem: ide sorolhatók a környezeti zavarok (légköri instabilitásból adódó zavarok, vihar, villámlás, stb.) nem szándékos emberi tevékenységből adódó zavarok (polgári rádióadások, mobiltávközlési zavarok, stb.), és a szándékos zavarok is (elektronikai ellentevékenység). A szándékos zavarok kiküszöbölésének vannak hardveres és szoftveres megoldási lehetőségei, illetve egyszerűbb, az eszköz kialakításával megoldható módszerei. Véleményem szerint a speciális terepi kivitel megvalósításába csak az utóbbi módszer értendő, az első kettő az elektronikai védelem témakörébe tartozik inkább.

Speciális terepi követelmények megvalósítása:

Az eszközök robosztusságának, külső hatásokkal szembeni ellenálló képességének biztosítása általában valamilyen speciális borítás alkalmazásával történhet (rázkódás ellen valamilyen zselés anyag használata, elektromágneses zavarok ellen megfelelő fémborítás alkalmazása, ütésállóságra megfelelő keménységű, vagy éppen megfelelő rugalmasságú bevonat használata, leejtés ellen csúszásgátló bevonat – például gumi – alkalmazása, stb.). A környezeti hatások közül néhány esetében nem a külső bevonat, hanem a megfelelő illesztések, tömítések, szigetelés használata jelent védelmet, míg a magas, vagy alacsony hőmérséklet ellen hűtő-, fűtőberendezésekkel, vagy megfelelő hőszigeteléssel lehet védekezni.

3.2. Szenzorhálózatoknál releváns terepi követelmények

A szenzorokat tartalmazó node-ok esetében a fent felsorolt hatások közül a környezeti hatásokkal és az elektromágneses zavarokkal kell számolni. A felsorolt hatások közül szenzortípusonként, telepítési helyenként más és más tekinthető relevánsnak, azonban a környezeti- és szándékos elektromágneses zavarokkal szemben mindegyiknek kell tartalmaznia valamilyen védelmet. Az emberi tényezőkkel itt nem kell számolni, illetve annak egy speciális értelmezését kell alkalmazni. Itt a leejtés, rázkódás, folyadékkal való leöntés nem fordulhat elő, viszont a célterületre történő kijuttatás jellemző módjaiból (tüzérségi löveg, repülőgépről kiszórás) fakadóan extrém ütés- és rázkódás elleni védelemmel kell ellátni a node-okat, hogy a célterületre érkezéskor a lehető legkisebb sérülés – vagy inkább semmilyen sérülés se – érje őket. A 3. táblázatban a fentieken túlmenően az egyes szenzortípusok helyes működéséhez szükséges jellemzők vannak sötét háttérszínnel jelölve.

	Hőmérséklet	**Köd**	**Por**	**Páratartalom**	**Domborzat**
Akusztikus					■
Szeizmikus					
Mágneses					
Elektro-optikai képi		■	■		■
Infravörös képi	■	■	■		■
Nyomás					
Rádiófrekvenciás rezgés					■
Kémiai/biológiai/nukleáris	■			■	
Mechanikai és infravörös		■	■		■
Meteorológiai					

3. táblázat. Releváns terepi környezeti hatások szenzortípusonként

A releváns terepi követelmények ezek alapján:

– Hőmérséklet-tűrés: fontos jellemző az a hőmérsékleti tartomány, amelyben a szenzorok képesek működni. Ezt a működési hőmérsékletet a levegő és a felszín hőmérséklete együttesen befolyásolja. A hőmérséklet-tűrés meghatározásakor figyelembe kell venni a technológiai korlátokat és a gyártási költségeket egyaránt,

ezért csak olyan hőmérsékletekre kell felkészíteni az eszközöket, amelyek a célterületen előfordulhatnak. A Földön a legalacsonyabb hőmérsékletet az Antarktiszon mérték (-89,2°C), a legmagasabb hőmérsékletet Líbiában (58°C), a legmagasabb felszínhőmérsékletet pedig Kaliforniában (93,9°C). Ezek a kiugró értékek leginkább olyan helyeken fordulnak elő, amelyek geológiai, állattani, vagy egyéb tudományos kutatások célpontjai lehetnek. Lakott területeken is előfordulnak hasonló hőmérsékletek (-71°C, Ojmjakon; 58°C, El Aziziya, Líbia), ami viszont a katonai felderítés esetén figyelembe veendő tényező. [7]

- Vízállóság: olyan területeken kell ezzel számolni, ahol eső is előfordul. Ez gyakorlatilag az állandóan fagypont alatt lévő területek kivételével a Föld egészére igaz. Van, ahol extrém esőzések fordulnak elő – például az esőerdőkben, ahol minden nap esik – és van, ahol csak az év bizonyos szakában fordul elő csapadék – például a sivatagokban, ahol a nyári esős évszakban esik jelentős mennyiségű eső. A vízállóság segíthet a magas páratartalom okozta problémák kiküszöbölésében is.
- Porállóság: fontos az eszközök elektronikájának védelme a portól, hogy az eszközt felépítő áramkörök hibátlanul tudjanak működni.
- Elektromos zavarokkal szembeni ellenálló-képesség: civilizált lakott területeken és azok környezetében nem szándékos zavarok a rádió- tv adások, mobiltávközlési eszközök miatt biztosan előfordulnak, lakott területeken kívül a nagyfeszültségű elektromos vezetékek okozhatnak hasonló zavart, és katonai alkalmazás esetén a szándékos zavarással is számolni kell.
- Nem kiküszöbölhető zavarok: a köd, por, és domborzat által okozott problémák bizonyos szenzortípusok esetén a működést teljesen lehetetlenné teszik. Ilyenek az elektro-optikai eszközök. A domborzati viszonyok az egyes node-ok hálózatba kapcsolódását és egymással való kommunikációját is meghiúsíthatják. Ezek olyan zavarok, amelyek ellen semmilyen előre beépíthető védelem nem alkalmazható.

Az elektronikai eszközök borításának vízállóságra és porállóságra vonatkozó szabványt dolgozott ki az International Electrotechnical Commition, IEC 60529-es szám alatt. Ebben definiáltak egy kódrendszert, amelyben a porállóság 0-6, a vízállóság pedig 0-8 közötti skálán értelmezettek. A kód „IP xy" formájú, ahol x a porállósági, y pedig a vízállósági érték. A 4. táblázat tartalmazza az egyes kódok jelentését.

IP xy			**Vízállóság (y)**								
Porállóság (x)		**Idegen tárgy elleni védelem (tárgy átmérője)**	**Nincs**	**Függőle-gesen cseppenő víz**	**Függőleges ±15°**	**Függőleges ±60°**	**Fröccsenő víz minden irányból**	**Kisnyomá-sú vízsugár**	**Erős vízsugár**	**Vízbe merí-tés**	**Víz alatti műkö-dés**
0	**Nincs**		IP 00								
1	**>50 mm ∅**		IP 10	IP 11	IP 12						
2	**>12,5 mm ∅**		IP 20	IP 21	IP 22	IP 23					
3	**>2,5 mm ∅**		IP 30	IP 31	IP 32	IP 33	IP 34				
4	**>1 mm ∅**		IP 40	IP 41	IP 42	IP 43	IP 44				
5	**por (részleges)**		IP 50				IP 54	IP 55			
6	**por (teljes)**		IP 60					IP 65	IP 66	IP 67	IP 68

4. táblázat. IP kódok az IEC 60529 szabvány szerint [8]

A porállóságnak és vízállóságnak általánosságban a műanyagok, illetve bizonyos fémek tesznek leginkább eleget. Az Altech cég az általa gyártott eszközök hőállóságáról és kémiai anyagokkal szembeni ellenálló-képességéről is közölt táblázatokat a technikai leírásban, amelyből készítettem egy összefoglalót a szenzorhálózatoknál releváns paramétereket felhasználva (5. táblázat). A kémiai anyagok közül azokat vettem figyelembe, amelyek egy terepen elhelyezett szenzor esetén relevánsak lehetnek. Gyenge sav a savas esőkből, benzin, gázolaj az esetlegesen elhaladó járművek üzemanyagaként, ásványi olaj a járművek motorjának kenőolajaként, ammónia pedig állati vizeletben, vagy növényi részek bomlásakor keletkezhet. A táblázatban megadott hőmérséklet-tartományban az anyagok megőrzik vízállóságukat és porállóságukat.

Az itt felsorolt anyagok közül az alumínium a legellenállóbb a kémiai anyagokkal szemben, és hőmérséklet-tűrése is a legjobbak közé tartozik, azonban elektromos szigetelő- és hőszigetelő képessége csekély, illetve nem rendelkezik ilyen tulajdonságokkal. A táblázatban található műanyagok közül mindegyik a hőre lágyuló műanyagok közé tartozik. Ezek közül az elasztomer, a polietilén, poliuretán és polipropilén minden kémiai anyaggal szemben részlegesen, vagy teljesen ellenállóak, és elektromos, illetve hőszigetelő képességük is jó.

Anyag	Hőmérséklet-tartomány (°C)	Víz	Gyenge sav	Benzin	Ásványi olaj	Gázolaj	Ammónia	Elektromos szigetelő	Hőszigetelő
Polisztirol	**[-25;+40]**	●	●	○	◒	○	●	●	●
ABS	**[-25;+40]**	●	●	○	●	●	○	●	●
Üvegszálas polikarbonát	**[-35;+80]**	●	●	●	●	◒	○	●	●
Polikarbonát	**-**	●	●	●	●	◒	○	●	●
Átlátszó polikarbonát	**[-35;+80]**	●	●	◒	●	◒	○	●	●
Hőre lágyuló elasztomer	**-**	●	●	◒	◒	◒	◒	●	●
Polietilén	**-**	●	●	◒	◒	◒	●	●	●
Poliuretán	**-**	●	◒	◒	●	◒	◒	●	●
Alumínium	**[-35;+75]**	●	●	●	●	●	●	○	○
Polipropilén	**[-25;+40]**	●	●	◒	●	◒	●	●	●
● - ellenálló / szigetelő	**◒ - részben ellenálló / szigetelő**	**○ - nem ellenálló / szigetelő**							

5. táblázat. Hőállóság és kémiai anyagokkal szembeni ellenálló-képesség [8]

4. TEREPI KÖVETELMÉNYEK MEGVALÓSÍTÁSA

4.1. Terepi követelmények megvalósítása szenzorhálóztatokban

Kutatásaim alapján azt a következtetést vontam le, hogy a manapság gyártott szenzor node-ok többsége fel van készítve extrém, vagy a normálisnál zordabb környezeti hatások elviselésére még a nem katonai célú szenzorok esetén is. Két gyártó termékeit emelem most ki: az egyik a Dust Networks, a másik pedig a MicroStrain.

A Microstrain két termékcsaládot gyárt: az egyik a Wireless Thermocoule Sensors, a másik a Wireless Sensors. Mindkét család node-jaiban található hőmérséklet-érzékelő, rádió a kommunikációhoz, a Wireless Thermocouple családnál extrém hőmérsékletek mérése is

lehetséges, ezen kívül relatív páratartalmat is képes mérni. A Wireless Sensors család csak normál hőmérsékleti tartományú hőmérséklet-méréseket tud végezni, és felszerelhetőek opcionálisan gyorsulásérzékelővel is.

Wireless Thermocouple Sensors jellemzők:

- 3 különböző node-típust foglal magába;
- Működési hőmérséklet: [-20°C; +60°C] normál akkumulátorral és borítással, [-40°C; +85°C] speciális akkumulátorral és borítással;
- Energiaforrás: Li-ion akkumulátor 550-650 mAh;
- Élettartam: a mintavételi sűrűségtől függően 23 nap – 10 hónap;
- Borítás: ABS műanyag (Akrilnitril Butadién Sztirol);

Wireless Sensors jellemzők:

- 4 különböző node-típust foglal magába;
- Működési hőmérséklet: [-20°C; +60°C] normál akkumulátorral és borítással, [-40°C; +85°C] speciális akkumulátorral és borítással;
- Energiaforrás: Li-ion akkumulátor 250 mAh, 600 mAh;
- Borítás: ABS műanyag (Akrilnitril Butadién Sztirol);

Láthatóan itt az extrém körülmények közül a hőmérsékletre készítették fel a szenzorokat. Már az alapfelszereltség is tekintélyes hőmérsékleti tartományban képes működni az afrikai sivatagi körülményektől az európai kemény telekig. Ezt a manapság a híradástechnikai eszközöknél, illetve a hangszerkészítésben is széles körben elterjedt ABS műanyaggal valósították meg. Az extrém borításról nem található információ a leírásokban, de valószínűleg valamilyen plusz hőszigetelő réteget használnak az ABS mellett. [9]

A Dust Networks cég SmartMesh termékcsaládjának tagjai is hasonló paraméterekkel rendelkeznek, itt azonban az áramköri panelek nincsenek külső borítással ellátva, ennek ellenére ugyanolyan hőmérsékleti tartományban képesek ellátni feladatukat. Az egyes termékcsaládok egymástól leginkább az ajánlott felhasználási területben és a felhasznált vezeték nélküli technológiában térnek el. Kiemelendő ezek közül a SmartMesh WirelessHART M2510 típusjelzésű node, amelyet gyári extrém körülményekre terveztek, alkalmazva az IEC 60770-1 magasvibrációs-tesztet és ellenőrizve ezzel a node ellenálló-képességét nagy vibrációs terhelés esetén. [10]

5. KATONAI FELHASZNÁLÁSRA GYÁRTOTT SZENZOROK TEREPI JELLEMZŐI

MCQ iScout Low Cost Remote Sensor [11]

A gyártó határvédelemre, épületeken belüli behatolás elleni védelemre ajánlja ezt a több szenzort, és hordozható monitorozó egységet tartalmazó rendszert.

- GPS vevő
- Szeizmikus, akusztikus, mágneses, passzív infra szenzorok
- Rádiófrekvenciás kommunikáció
- 14 napos akkumulátor-élettartam, külső energiaforrással 3 hónap-3 év élettartam
- Vízálló borítás
- Működési hőmérséklet: [-40°C; +60°C]

1. ábra. MCQ iScout Low Cost Remote Sensor [11]

MSQ OmniSense Imaging Sensor Unit [12]

- Automatikus jármű- és személyzet-detektálás és térképes megjelenítés
- Szeizmikus, akusztikus, mágneses és passzív infra érzékelők
- Rádiófrekvenciás, és műholdas kommunikáció
- Alacsony fogyasztás és hosszú élettartam
- A borításról és működési hőmérsékletről nincsen adat a gyártó honlapján és az adatlapon.

2. ábra. MSQ OmniSense Imaging Sensor Unit [12]

MCQ OmniWatch [13]

- Éjszakai és nappali kamera
- Vezeték nélküli kommunikáció
- Automatikus célpont-felismerés
- Kicsi, könnyű és környezeti hatásokkal szemben ellenálló. Ennek megvalósításáról a gyártó honlapján és az adatlapon nem található információ

3. ábra. MCQ OmniWatch [13]

Az MCQ és más gyártók által készített szenzorok és szenzorhálózatok esetében sajnos nem található részletes leírás az eszközök technikai paramétereiről, működési környezetükről. A terepi követelményeknek való megfelelésről legtöbbször csak a „rugged" jelző olvasható, az ennek megvalósításához felhasznált anyagokról nincs információ. Valószínűsíthetően a szenzor node-ok borításaként alumíniumot, vagy hőre lágyuló műanyagot használnak. Mivel a hőre lágyuló műanyagoknak nagyon hasonlóak a tulajdonságai, sőt az optikai paramétereik is, ezért az eszközök adatlapján megadott működési hőmérséklet-tartományokból és a fotók alapján sem lehet megállapítani, milyen anyagot használtak a gyártáshoz.

6. KONKLÚZIÓ

A szenzorhálózatokat egyre szélesebb körben használják az ipari gyártásban, katasztrófavédelemben, határvédelemben és a harcászati felderítésben egyaránt, mivel emberi erőforrás használata nélkül teszi lehetővé egy meghatározott célterület megfigyelését

A cikkben bemutattam a szenzorhálózatokkal kapcsolatos terepi követelményeket. A szenzorhálózatokkal kapcsolatos alapismeretek (szenzorok fogalma, típusai, jellemzői, szenzorhálózat fogalma, elemei, ad hoc hálózat fogalma) után csoportosítottam a szenzorhálózatokat. Majd bemutattam az általános, és a szenzorhálózatokra vonatkozó terepi követelményeket és végül elemzem a terepi követelmények megvalósításait.

Felhasznált irodalom

[1] Völgyesi Péter: Szenzorhálózatok, http://www.volgy.com/pubs/BIR_SensorNetworks.pdf; (letöltés: 2011. 11. 04.)

[2] Zsolt Haig: Networked unattended ground sensors for battlefield visualization, AARMS Vol. 3, No. 3, 2004, pp. 387-399

[3] R.C. Turner, P.A. Furierer, R.E. Newnham, T.R. Shrout: Materials for high temperature acoustic and vibration sensors: A review, Applied Acoustics Volume 41, Issue 4, 1994, pp. 299-324

[4] T. Bratland, M.J. Caruso, R.W Schneider, C.H. Smith: A New Perspective in Magnetic Field Sensing, 1998. http://www.sensorsmag.com/sensors/electric-magnetic/a-new-perspective-magnetic-field-sensing-855; (letöltés: 2011. 12. 20.)

[5] Buttyán L., Holczer T., Schaffer Péter: Kooperációra ösztönző mechanizmusok többugrásos vezeték nélküli hálózatokban, Híradástechnika LIX. évfolyam, 2004/3. http://crysys.hu/publications/files/ButtyanHS06ht.pdf; (letöltés: 2011. 12. 20.)

[6] Munk Sándor: Katonai Informatika III., A katonai informatika eszközrendszere. Egyetemi jegyzet, ZMNE, Budapest, 2003

[7] Meteorológiai világ- és kontinens rekordok, OMSZ, http://www.met.hu/omsz.php?almenu_id=misc&pid=met_rekordok&pri=1&mpx=1&stt=vilagrekordok; (letöltés: 2011. 12. 27.)

[8] Altech Technical Innex http://www.altechcorp.com/PDFS/TECHsp.PDF; (letöltés: 2011. 12. 27.)

[9] MicroStrain Wireless Sensor Networks, Sensors, http://www.microstrain.com/wireless/sensors; (letöltés: 2011. 12. 21.)

[10] Dust Networks, http://www.dustnetworks.com/products; (letöltés: 2011. 12. 21.)

[11] iScout Low Cost Remote Sensor, Datasheet, http://www.mcqinc.com/pdf/iScout_Datasheet-12-Jul2011.pdf; (letöltés: 2011. 12. 26.)

[12] OmniSense Imaging Sensor Unit, Datasheet, http://www.mcqinc.com/pdf/OmniSense-Datasheet-July_2010.pdf; (letöltés: 2011.12.26.)

[13] OmniWatch Datasheet, http://www.mcqinc.com/pdf/OmniWatchOnePageDatasheet_11-Aug2011.pdf; (letöltés: 2011.12.26.)

[14] ThermalScene Thermal Imagery 24/7, Datasheet, http://www.mcqinc.com/pdf/ThemalScene_datasheet.pdf; (letöltés: 2011. 12. 26.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Papp Zoltán
pappz.szeged@gmail.com

A HELYZET-MEGHATÁROZÓ RENDSZEREK ZAVARÁSA

Absztrakt

Különböző tárgyak, vagy akár saját térbeli elhelyezkedésünk pontos ismerete az információs társadalom számos katonai, rendészeti, vagy akár gazdasági folyamatában tölt be fontos szerepet. A helyzet-meghatározó rendszerek jelentőségükből adódóan fokozottan ki vannak téve a különböző indíttatású támadók tevékenységének.

The exact knowledge of the geographical position of various objects or even ourselves has an important role in military, law enforcement or even economic processes of an information society. Due to their significance, positioning systems are highly exposed to the activities of attackers with various motives.

Kulcsszavak: *helyzet-meghatározás, kritikus információs infrastruktúra, információs terrorizmus, elektronikai zavarás ~ positioning, critical IT infrastructure, IT terrorism, electronic jamming*

1. BEVEZETŐ

Térbeli elhelyezkedésünk meghatározására – döntően katonai szempontok alapján – több eljárást is kidolgozásra került a hidegháború időszakában. A szembenállás elmúltával a katonai helyzet-meghatározó rendszerek által nyújtott szolgáltatások egyre szélesebb körű alkalmazást nyertek a polgári életbe is. Az elektronikai eszközök, miniatürizálódásával, képességeik fejlődésével ezek a szolgáltatások már a privát és a gazdasági szektor egyre több folyamatába integrálódtak, olykor meglepő helyen, funkcióban bukkannak fel [1]:

- Közlekedés - áruszállítás
- Kereskedelem
- Földmérés - térinformatika
- Környezetvédelem
- Időszinkronizálás
- Emberi élet védelme
- Katasztrófa-elhárítás
- Mezőgazdaság
- Távközlés
- Egyéb

A technológia katonai jellegű alkalmazási céljai egyértelműek, fő felhasználási módjai a saját vagy ellenséges csapatok elhelyezkedésének nyomon követése, illetve a fegyverirányítási rendszerek hatékonyságának növelése köré csoportosíthatóak. A polgári életben felhasználásuk lényegesen sokrétűbbnek tekinthető. A felhasználói kör szélesedésének egyik oka lehet az, hogy az elektronikai – főleg a kommunikációs – eszközök gyártói helyzet-meghatározásra alkalmas chipkészletekkel szerelik fel termékeiket, és speciális alkalmazások telepítésével egyfajta mesterséges igényt teremtve szolgáltatás iránt a vásárlók körében. A gazdasági szektor szereplői lényegesen tudatosabban, tervezettebben, racionális megfontolások alapján, gyakorlatilag a működés hatékonyságának és a szolgáltatás biztonságának növelése érdekében használják fel a helyzet-meghatározási technológiák által nyújtott lehetőségeket. Például hatékony és gazdaságos irányítás érdekében jöttek létre flotta-követési megoldások, ahol nyomon lehet követni a mozgásban lévő járműpark földrajzi elhelyezkedését, kihasználtságát és különböző optimalizációs eljárásokat alkalmazva dinamikusan be lehet avatkozni a munkafolyamatokba. A pontos földrajzi elhelyezkedés ismeretéből adódó előnyöket nem csak a privát és a gazdasági szektor tudja felhasználni, mivel léteznek olyan állami funkciók is, melyekben szintén fontos szerepet tölt be a helyzet-meghatározás.

A helyzet-meghatározás, illetve az ezen alapuló szolgáltatások nagyfokú elterjedésével az információs társadalom szereplői e téren is kiszolgáltatottá váltak egy információs infrastruktúra irányába. A helyzet-meghatározás lehetőségének átmeneti, vagy tartós zavara esetén a ráépülő szolgáltatások is kiesnek, melyek az interdependencia okán más szolgáltatásokat is érinteni fognak.

Jelentőségéből adódóan kézenfekvő, hogy a bizonyos helyzetekben (például háborúk, terrorcselekmények, bűncselekmények esetén) a helyzet-meghatározó rendszerek kiemelt célpontjai lehetnek támadóknak.

2. KIALAKULÁSUK

Az emberiség történelmében, bolygónk felfedezése során, a hosszú hajóutakon, a Nap és más csillagok égen történő elhelyezkedése alapján tájékozódtak a hajósok a tengeren. A navigációs eszközök fejlődésével a helymeghatározás egyre pontosabbá vált, azonban a rádiótechnika, majd a műholdak megjelenése hozta el a valódi forradalmat. Az első rádió-

navigációs rendszer kifejlesztésének ötlete már az első világháborút követően felvetődött, aminek segítségével a hajók navigátorai meghatározhatták a helyzetüket partközelben. A LORAN (Long Range Aid to Navigation) elnevezésű rendszert az amerikai hadsereg a második világháború kezdetekor már rendszerbe állította. A LORAN hálózat elérhető volt a világ legtöbb helyéről, főleg Európából és Amerikából, azonban csak kétdimenziós rendszer volt, s ez által, nem volt alkalmas repülőgépek helyzet-meghatározására [2].

A műholdak első generációjának megjelenésekor megfigyelték, hogy a műholdról kibocsátott rádiójelek hullámhosszának változását elemezve meg lehet határozni a műhold helyzetét. A lehetőség felhasználása érdekében először az Egyesült Államok haditengerészetének kutatólaboratóriuma 1958-ban megkezdte saját navigációs rendszerének kifejlesztését. A tervezésnél követelményként fogalmazták meg, hogy a passzív módban működő navigációs vevőberendezések pontosságának 0,1 tengeri mérföldnél jobbnak kell lennie, illetve a rendszernek folyamatos üzeműnek kell lennie. A fejlesztés eredményeképpen 1964-re kiépítették a TRANSIT nevű rendszert, mely a haditengerészet hajóegységeinek, továbbá a ballisztikus rakéták navigációját segítette. A TRANSIT rendszer négy kis méretű műholdból állt, melyek Föld körüli poláris pályán ezer kilométeres magasságban keringtek. A felhasználó egységek a doppler-effektus segítségével – néhány óránként – percek alatt meg tudták határozni földrajzi helyzetüket. A TRANSIT rendszer – több modernizáción átesve – egészen 1996-ig használatban maradt, amikor is felváltották az új generációs navigációs műholdak [3].

Az idők folyamán több különböző típusú (kontinentális, globális) és célú helyzet-meghatározó rendszer került kifejlesztésre, azonban ezek közül alig néhánynak sikerült szélesebb felhasználói kört maga köré gyűjtenie, de ezek közül kiemelkedik az amerikai Navstar GPS rendszer, amellyel háromdimenziós helyzet-meghatározást végezhetünk földön, vízen vagy levegőben. Ez a technológia – számos más megoldáshoz hasonlóan – először katonai célokra lett kifejlesztve, de ma már jelen van a polgári élet szinte minden területén is. A kereskedelmi forgalomban elérhető vevőkészülékek pontossága jellemzően méteres nagyságrendű, de speciális vevőkészülékekkel és differenciális mérési módszerekkel pontossága – valós időben – akár milliméteres nagyságrendre is képes.

3. A GPS RENDSZER

A Rockwell International vállalat által kifejlesztett Navstar GPS (Navigation System with Timing and Ranging Global Positioning System) helyzet-meghatározó rendszer működésének elveit 1973-ban fektették le. Követelmény volt, hogy minden napszakban, időjárás körülmények és légköri viszonyok között működnie kellett, függetlenül a földfelszíntől mért távolságtól és a mozgási sebességtől.

A helyzet-meghatározó rendszer huszonnégy műholdból épül fel, melyek a Föld felszínétől 20200 kilométeres magasságban keringenek. A műholdak keringési ideje 11 óra 58 perc, hat pályasíkon helyezkednek el, egymáshoz képest 60 fokkal elforgatva, pályasíkon-elhajlásuk az egyenlítőhöz képest 55 fokos. A műholdak elhelyezkedése olyan, hogy minden pillanatban a Föld bármely pontjáról bármely pillanatban legalább négynek látszódnia kell. A Navstar GPS rendszer működését a Colorado Springs-be telepített földi vezérlőrendszer irányítja, mely kiegészül négy monitorállomással (Hawaii, Kwajalein, Diego Garcia, Ascension Island) is. A földi vezérlőegység a következő feladatokat látja el:

- a műholdak működésének folyamatos figyelése, az egyes egységek állapotának ellenőrzése;
- a műholdak pályaadatainak folyamatos mérése, a műholdon tárolt adatok frissítése;
- a műhold fedélzeti óráinak szinkronizálása, a pontos idő beállítása;

– a műholdon tárolt navigációs üzenettár frissítése, a helymeghatározáshoz szükséges korrekciós adatok (időjárási adatok, a légkör és az ionoszféra állapotjellemző) gyűjtése és továbbítása a műholdak felé.

A földi állomások sűrűségének növelésével növelhető a GPS rendszer pontossága.

A GPS műholdak két frekvencián sugározzák jeleiket, L1 (1575,42 MHz), illetve L2 (1227,6 MHz) csatornákon. Minden műhold szórt spektrumú jelet, úgynevezett pszeudo-véletlen zajt (pseudo-random noise: PRN) sugároz, és ez a jel pedig minden műholdnál különbözik. A PRN kódoknak két fajtája van:

C/A - kód (Coarse / Acquisition code - durva elérés kód), ami ezred másodpercenként 1023 jelet tartalmaz, azaz egy kódelem időtartama 1 μs.

P(Y) - kód (Precision code - pontos kód), ami 10230 jelet tartalmaz. Egy kódelem időtartama csak 0,1 μs.

A C/A kódot az L1 frekvencián adják, a P-kódot mindkét frekvencián. A P-kódot csak speciális katonai vevővel lehet dekódolni, ez kereskedelmi forgalomban nem hozzáférhető. Természetesen a pontossága lényegesen nagyobb, mint az általános, polgári célokra is használható C/A kódnak. 2000-ig az Egyesült Államok torzította a jelek vételét (SA - Selective Availability), így korlátozva a rendszer pontosságát, ezért a rendszert nem katonai jogosultsággal használók akár több száz métert is tévedhettek. A pontos jelet kizárólag a katonai jel vételével lehetett biztosítani, ehhez azonban a katonai vevőn túl az adott napi kódra is szükség volt. 2000-ben Bill Clinton elnök elrendelte az SA jel sugárzásának megszüntetését, de bármikor visszakapcsolható.

A GPS rendszer lényege a távolságmérés. A műholdaknak a vevőkészüléktől való távolsága egyszerűen a műholdak által kisugárzott jelek beérkezési idejéből számítható ki, ha pedig ismert néhány műholdtól való pontos távolság, valamint egy referenciapontként szolgáló műhold helye, akkor meghatározható a vevő pontos elhelyezkedése. Mivel a rádióhullámok fénysebességgel terjednek, így a nagy terjedési sebesség miatt nagyon pontos időmérésre van szükség. Ha a meghatározandó műhold zenitben van, akkor 0.06 másodperc alatt ér le a mérőjel róla, így a centiméteres mérési pontosság eléréséhez a vevő órájának 0.000000001 másodperc pontossággal kell mérnie.

4. KIEGÉSZÍTŐ FUNKCIÓK

A GPS technológiájához kapcsolódóan léteznek olyan kiegészítők, kényelmi funkciók is, melyek a rendszer alaprendeltetését, szolgáltatási portfólióját kibővítik. Egyik ilyen funkció a TMC (Traffic Message Channel) forgalmi információs vevő, mely FM csatornákon működik az RDS (Radio Data System) technológia alapján, és a valós idejű útvonaltervezés hasznos eleme. A TMC üzenetekben különféle hely-, esemény-, és időkódok sugároznak, amelyek időben és térben leírnak egy akadályt (például forgalmi dugót). Az üzenetekben jelzett akadály pozíciójának ismertében az útvonaltervezést végző készülék az útvonalat valós időben, dinamikusan és automatikusan áttervezi. A digitalizált és kódolt, valós idejű forgalmi adások egy rádióállomás RDS csatornáján kerülnek továbbításra, így a felhasználó továbbra is bármiféle zavarás nélkül képes hallgatni a rádióadókat. A TMC funkció passzív megoldásnak tekinthető, mivel pontossága a rádiócsatornát üzemeltető információihoz kapcsolódik. Magyarországon a TMC szolgáltatáshoz szükséges jelet a Magyar Rádió sugározza, a Fővinform és az Útinform információi alapján (kiegészülve 5000 gépjárműbe szerelt eszközzel - FCD), Budapesten 800 csomópontot és eseményt figyelnek, országosan 2300-at.

Dinamikusabb útvonaltervezés valósítható meg, ha a felhasználók interaktívan részt vesznek a forgalmi helyzet felmérésében. Az FCD (Floating Car Data) rendszerben minden autó egy-egy anonim közlekedési szenzorként szolgál, melynek alapját egy fedélzeti helyzet-meghatározó berendezés és egy mobilkommunikációs eszköz képezi. A helyzet-meghatározó

berendezés kiszámítja a jármű pillanatnyi sebességét és helyét, majd bizonyos időközönként mobilkommunikációs eszközön keresztül elküldi az információkat a központba. Minél több jármű vesz részt ebben a FCD rendszerben, annál jobban látható az aktuális közlekedési helyzet. A szolgáltatásban részt vevő navigációs készülékek felhívják a központot, megadják tervezett útvonalukat, majd tájékoztatást kapnak a jelzett útvonal pillanatnyi közlekedési helyzetéről, és akadályok esetén áttervezik azt egy alternatív menetvonalra.

5. A HELYZET-MEGHATÁROZÁSSAL KAPCSOLATOS SZOLGÁLTATÁSOK TÁMADÁSA

Tekintettel arra, hogy a helyzet-meghatározást lehetővé tevő infrastruktúrák által nyújtott szolgáltatások mind katonai, mind pedig polgári felhasználási lehetőségei igen szélesek, ami közül néhány kiemelt fontosságú, így ezek megszűnése, hosszabb-rövidebb ideig tartó zavara jelentős hatással lehet a társadalom egyes funkcióira. A felhasználási lehetőségek között vannak olyanok, melyek esetében a szolgáltatás kiesése nem jelent kritikus fennakadást, azonban vannak olyan elemek, melyek esetében a kiesés azonnali zavart okoz, vagy okozhat. Geodéziai célú felhasználásakor a szolgáltatás kiesése nem okoz fennakadást, mivel például a földrészek mozgásának nyomon követése akár hónapokat is szünetelhet. Mezőgazdasági célú alkalmazások esetében az információs infrastruktúra üzemzavara azonban – az adott agrikultúra jellegétől függően – már csak napokban tolerálható. Vannak azonban olyan tevékenységek is, melyekben a helyzet-meghatározási szolgáltatások kimaradása azonnali fennakadást, zavart, gazdasági kárt, vagy akár veszélyt okoz. E körben kiemelhető közszolgáltatás a repülésirányítás, a katasztrófa-elhárítás támogatása, vagy épp a fegyverirányító rendszerek számára szükséges információk biztosítása. A gazdasági szektor vonatkozásában kiemelhetők a flottakövetési, vagyon- és személyvédelmi szolgáltatások, melyekre szinte azonnali hatással lehetnek az üzemzavarok, amik gazdasági károkat is okozhatnak.

Az érintett infrastruktúrák fontosságukból adódóan fokozottan ki vannak téve az ártó szándékú tevékenységeknek, melyek mögött különböző motivációk húzódhatnak meg. Mivel ezek az infrastruktúrák alapvetően katonai célok érdekében jöttek létre, így értelemszerűen háborús körülmények között az ellenség egyik kiemelt célpontjai.

A NavStar GPS helyzet-meghatározó rendszer esetében az infrastruktúrára az ellenséges fegyveres erők jelenthetik a legnagyobb veszélyt, mivel az ő birtokukban lehetnek meg azok az eszközök (rakéták, EMP), melyek képesek az űrbe telepített műholdakat, vagy a földi állomásokat elpusztítani. A fizikai pusztításhoz szükséges eszközrendszerek hiányában hatékony módszer a műholdak által sugárzott jelek zavarása, annak érdekében, hogy a vevőkészülékek ne legyenek képesek azt feldolgozni. Ez az eljárás mód szintén a hadseregek által alkalmazva érhet el maximális hatékonyságot (földrajzi terület nagysága, jelerősség), mivel az ő eszközparkjában léteznek a megfelelő elektronikai hadviselési rendszerek, azonban ezek a zavaróeszközök – kisebb hatékonysággal ugyan – kereskedelmi forgalomban is megvásárolható alkatrészekből is előállíthatóak, így a potenciális felhasználók köre igen széles lehet.

A helyzet-meghatározó rendszerek a bűnözés oldaláról is ki vannak téve az ártó szándékú tevékenységnek. Ez irányból az infrastruktúraelemek támadásának veszélye elhanyagolható, mivel ennek a körnek nincs a megfelelő eszközrendszere ahhoz, hogy a védett elemekre valódi fenyegetést jelentsenek, azonban a szolgáltatások minőségére képesek oly mértékű hatás gyakorolni, hogy céljaikat elérjék. A bűnözői körök a különböző vagyon- és személyvédelmi célú szolgáltatások (GPS-s gépjárművédelem, pénzszállítás, házi őrizetbe helyezett személyek nyomon követése, stb.) akadályozása kapcsán merülhetnek fel, mint támadók.

A helyzet-meghatározó rendszerek, illetve az általuk nyújtott szolgáltatások megbénítása nem csak az ellenséges hadviselő felek, vagy bűnözők célja lehet. Zavar- vagy pánikkeltés, gazdasági károkozás érdekében a terroristák célpontjaivá is válhat egy adott rendszer. A GPS infrastrukturális elemei az ő számukra is elérhetetlenek, azonban a szolgáltatás manipulációjával hatékonyan tudnak beavatkozni az információs társadalom életébe. A TMC vagy az FCD funkciók átírásával a közutakon közlekedési káoszt tudnak elérni, vagy a GPS jelek zavarásával, módosításával képesek veszélyeztetni a légi- és a vasúti közlekedést, vagy akár veszélyes anyagok szállítását is. Ez a fajta támadásmód pedig kifejezetten vonzó is lehet számukra, mivel – a számítógép-hálózatokon keresztül történő támadásokhoz hasonlóan – a felhasznált zavaróeszközök távolról, akár távirányítással és tömegesen is bevethetők, ami jelentősen csökkenti az általuk vállalt kockázatot.

Mivel a GPS által kisugárzott jelek rendkívül kis teljesítményűek (-130 dBmW), így már egy kis teljesítményű (10^{-12} W) interferencia forrás is elegendő a jelek értelmezhetetlenné tételéhez. A GPS műholdak nemzetközileg védett frekvenciákon sugározzák jeleiket, tehát tilos ugyanezen sávokban bármilyen más jelet sugározni, így az esetleges zavarást könnyű érzékelni. A GPS szolgáltatások használhatatlanságának több oka lehet [1].

Nem szándékos zavarás esetén a szolgáltatás minőségét természeti jelenségek, vagy nem szándékos emberi tevékenységek is zavarhatják:

- az ionoszféra okozta interferencia:
  - Ionoszférikus jelkésleltetés. A műholdak által sugárzott jelek teljes pályájuk mentén az elektromágneses sugárzás vákuumbeli terjedési sebességével haladnak. A műholdak pályamagassága miatt a jelek az útjuk nagy részét vákuumban teszik meg, de a vevőbe érkezésük előtt áthaladnak a földi légkörön, miközben sebességük nem elhanyagolható mértékben csökken [4].
  - Szcintilláció. A légkör lokális elektronsűrűségének változásából adódó gyors amplitúdó és fázisváltozások a jelben.
- Rádióforrások okozta nem szándékos interferencia. Mivel a GPS jelek rendkívül kis teljesítményűek, így könnyű megzavarni egy ugyanabban a mikrohullámú sávban működő nagyobb teljesítményű rádióadóval (URH adók, szélessávú radar és kommunikációs berendezések, stb.).

Szándékos zavarás esetei:

- Jamming: Megfelelő energiájú és megfelelő spektrális összetételű zavaró jelek kibocsátása interferenciát okoz, így a műholdak által kisugárzott jelek a vevőkészülékek számára értelmezhetetlenné válnak. A zavarjel típusa lehet keskeny- vagy szélessávú folyamatos adás, vagy pedig szórt spektrumú, a GPS jelhez hasonló. Egy 1 wattos zavaróadó folyamatos adásmódban 10 kilométeres hatótávon belül a vevőkészület leszakítja a műholdak jeléről, 70 kilométeren belül pedig megakadályozza azt, hogy felvegyen egy új műholdat. Szórt spektrumú adásmódban az 1 wattos zavaróadó 1000 kilométeres távolságig alkalmazható.
- Spoofing: A vevőkészülék megtévesztése érdekében megfelelő energiájú, valódinak látszó C/A jelek kisugárzása, így a vevőkészülék a kívánt pozíció irányába eltéríthető.
- Meaconing: A műholdak által kisugárzott jeleket rögzítik, majd bizonyos idővel késleltetve, megfelelő energiával újrasugározzák őket, így összezavarják a vevőkészüléket.

A nagyteljesítményű, professzionális, általában katonai GPS zavaró berendezések többféle zavarójel kibocsátására képesek, azonban ezek viszonylag könnyen bemérhetők és elpusztíthatók. Az alacsony teljesítményű, kisméretű zavaró készülékek (1. ábra) egyszerű

felépítésűek, kereskedelmi forgalomban is elérhető alkatrészekből megépíthetőek, ezért olcsók, ami elősegítheti nagyfokú elterjedésüket, és esetlegesen tömeges alkalmazásukat.

1. ábra. Kisméretű zavaróeszközök
Forrás: http://www.agt.bme.hu/tantargyak/gpselm/eloadas/HT_26apr.pdf;
http://www.foxnews.com/scitech/2010/03/17/gps-jammers-easily-accessible-potentially-dangerous-risk/;

Az alacsony teljesítményű, kisméretű zavaró berendezések elleni küzdelmet nehezíti, hogy a felhasználás jellegéből adódóan viszonylag rövid ideig üzemelnek (például egy jármű eltulajdonításánál néhány órát), ami sok esetben még a zavarás tényének megállapításához sem elegendő. A zavaróadó bemérése érdekében a mérőeszközöket pedig viszonylag közel kell telepíteni, amit a támadó észlelhet.

6. A GPS-ZAVARÁS EDDIGI ESETEI

Az Egyesült Államok fegyveres erői háborús konfliktusaiban fokozottan támaszkodtak a fejlett navigációs rendszerben rejlő lehetőségekre, ezért számítani lehetett arra, hogy a kibernetikus hadszíntéren előbb-utóbb megjelennek azok az eszközök, melyek a GPS nyújtotta előnyöket próbálják meg lerontani.

A második Öböl-háború ideje alatt az iraki hadseregben már meg is jelentek az első orosz fejlesztésű GPS-zavaró rendszerek, melyekkel korábban még nem találkoztak az amerikaiak. Az eszközök alkalmazása a háború kimenetelére nem volt jelentős hatással, azonban az orosz-amerikai politikai kapcsolatokat befolyásolta. Az orosz zavarórendszerek lelepleződése után az amerikaiak a következő GPS műhold-generációkat (Block-IIR-M) új, jobban titkosított, erősebb zavarvédelemmel, úgynevezett M kóddal látják el [5].

Az Egyesült Államokkal folyamatosan szembenálló Irán, hogy a technológia által nyújtott, számukra nem előnyös lehetőségeket adminisztratív intézkedésekkel igyekszik korlátozni, a szolgáltatások elérhetőségét bizonyos helyeken magánszemélyek és gazdasági társaságok számára kötelezően telepítendő zavaró-berendezésekkel akadályozza.

A távol-keleti térségben Észak-Korea – saját biztonságára hivatkozva, főleg az amerikai - dél-koreai hadgyakorlatok idején – rendszeresen zavarja a GPS műholdak jelét, ami Dél-Koreában, főleg a fővárosban, Szöulban okoz fennakadásokat. [6]

7. ÖSSZEGZÉS

A helyzet-meghatározó rendszerek által nyújtott szolgáltatásokra az információs társadalom számos funkciója épül, így kritikus információs infrastruktúrának tekinthető. Fontosságára való tekintettel számítani kell arra, hogy különböző motivációjú támadók különböző eszközökkel igyekeznek majd a rendszer működését befolyásolni. A veszélyt fokozhatja az, hogy a zavaróeszközök egyszerűségükből és alacsony költségükből adódóan széles körben elterjedhetnek (akár interneten is megrendelhetők), és tömeges alkalmazásuk nehezíti, vagy akár el is lehetetleníti az ellenük való harcot. A védekezés egyik módja lehet

az, hogy a helyzet-meghatározó eszközök zavarására, manipulálására alkalmas berendezések birtoklásának tilalmát törvénybe foglalják, ami azonban csak a zavarást kipróbálni szándékozók ellen nyújthat hatékony védelmet, mivel a szándékos, rosszindulatú támadókat ez nem fogja visszatartani. A manipulációk elleni védekezési mód lehet még az olyan intelligens vevőkészülékek tervezése, melyek a jelek – abszolút, relatív – erősségének változásaiból képesek érzékelni a manipulálási kísérletet.

A NavStar GPS hegemóniáját megtörni látszik, hogy az elkövetkezendő időszakban több műholdas navigációs rendszer (Glonass, Galileo, Beidou) is elérhetővé fog válhat a polgári felhasználás számára is, ami megfelelő – több típusú navigációs rendszer vételére alkalmas – vevőkészülékek esetén növeli a szolgáltatások biztonságát, mivel az egyik rendszer akadályoztatása esetén képes átállni egy másik navigációs rendszer vételére.

Felhasznált irodalom

[1] Horváth Tamás: "GPS Jamming" a GPS jelek szándékos zavarása (BME Általános és Felsőgeodéziai Tanszék, Egyetemi jegyzet 2005.)

[2] Loran-history.info website. http://www.loran-history.info/default.asp; (letöltve: 2011. 12. 06.)

[3] TRANSIT http://en.wikipedia.org/wiki/Transit_%28satellite%29; (letöltve: 2011. 12. 08.)

[4] Takács Bence: GPS-mérések abszolút feldolgozását terhelő hibahatások vizsgálata (Híradástechnika LIX Évfolyam 2004/5., p42, ISSN 0018-2028)

[5] GPS.gov weboldal. http://www.gps.gov/systems/gps/space/#IIRM; letöltve: (2011. 12. 06.)

[6] Észak-Korea zavarja a GPS-t? http://fn.hir24.hu/vilag/2011/03/06/eszak_korea_zavarja_gps; (letöltve: 2011. 12. 15.)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Szabolcsi Róbert
szabolcsi.robert@uni-nke.hu

UAV AUTOMATIKUS REPÜLÉSSZABÁLYOZÓ RENDSZER SZÁMÍTÓGÉPES TERVEZÉSE

Absztrakt

A légi robotok egyre szélesebb körben alkalmazott eszközök úgy a polgári, mint a katonai alkalmazások területén. A légi robotok repülésének számos fázisa automatizálható a kereskedelmi forgalomban is beszerezhető eszközök segítségével. Az UAV fedélzeti eszközök azonban utólagos hangolásra késztetik az alkalmazókat. A hangolások, az előzetes szabályozótervezések során számos módszer használható, mint a heurisztikus módszer, a szabályozók tapasztalati beállítása, analitikus módszerek, illetve számítógépes szabályozótervezés. Az UAVk közül a multirotoros légijárművek repülésszabályozásával foglalkozik a cikk. A quadrotor elrendezésű légijárművek függőleges tengely mentén történő mozgásának automatizálása biztosítja az automatikus magasságváltoztatás lehetőségét.

Robots are widely applied tools applied both in military and non-military missions. Leaning on theirs possibilities they allow executing missions impossible for human beings, i.e. in dangerous missions. The article deals with automation of he flight phases of the unmanned aerial vehicles (UAV). From large scale of available UAVs author will deal with multirotors. The spatial motion of the quadrotors will be investigated, and first solutions will be examined in vertical motion of the quadrotors.

Kulcsszavak: *katonai robotok, felderítő felszíni robotok, légi robotrendszerek, számítógépes tervezés ~ military robots, recce surface robots, air robot systems, CAD*

1. BEVEZETÉS, MOTIVÁCIÓ

A robotika, és a mechatronika legújabb tudományos eredményei alapján tervezett robotok katonai alkalmazása egyre szélesebb körű. A robotika területeiről a légi-, és a felszíni kutatórobotok alkalmazása már széleskörű, mindazonáltal a jelenlegi alkalmazási területeken kívül számos új alkalmazási terület is nyílik. A felderítő UAV alkalmazások során számos esetben merül fel a repülés automatizálásának szükségessége. Az automatizálás olyan távlatokat nyit, amelyeket az ember nem képes létrehozni. A repülésautomatizálás javítja az UAV stabilitási-, és irányíthatósági tulajdonságait, valamint megfelelő minőséget is biztosít. A repülés számos fázisa automatizálható, sőt, gyenge stabilitási jellemzőkkel bíró UAVk esetén ez szükséges is. A leggyakrabban automatizált repülési üzemmódok az Euler-szögek stabilizálása, pályavezérlő üzemmódok (pl. feszállás, leszállás, magasságstabilizálás, sebességstabilizálás). A cikkben a szerző olyan repülési fázis automatizálását veszi górcső alá, amely légi felderítés esetén különösen fontos. Ez az üzemmód a multirotoros UAV függésének szabályozása. Ezen üzemmódon a repülési magasság állandó értéken tartása a szabályozás célja, míg a hossz-, és a kereszt-tengelyek mentén a koordináta-változás zérusértékű, míg a tranziens folyamatok során a minőségi jellemzők megegyeznek az előre definiált jellemzőkkel.

2. SZAKIRODALOM ÁTTEKINTÉSE, TUDOMÁNYOS ELŐZMÉNYEK

A légijárművek térbeli mozgásának matematikai modellezésével, valamint az automatikus repülésszabályozó rendszerek előzetes tervezésével az [1, 2] irodalmak foglalkoznak. Pilóta nélküli repülőgépek katonai-, és nem-katonai alkalmazásának lehetőségeivel a szerző által publikált [3, 4, 5, 6, 7, 8, 9] cikkek foglalkoznak részletesen. A szerző a felhasználói oldalról mutatta be az UAV-kal szemben támasztott irányíthatósági-, kormányozhatósági-, és a stabilitási követelményeket. E minőségi jellemzők szabványa a [12] szabvány. Multirotoros (quadrotor) légijárművek mozgásának modellezésével, és a térbeli mozgásának automatizálásával a [10, 11] irodalmak foglalkoznak. A szerző bemutatta az optimális szabályozótervezés elméleti hátterét, és példán keresztül mutatta be a súlyozó mátrixok gyakorlati alkalmazását.

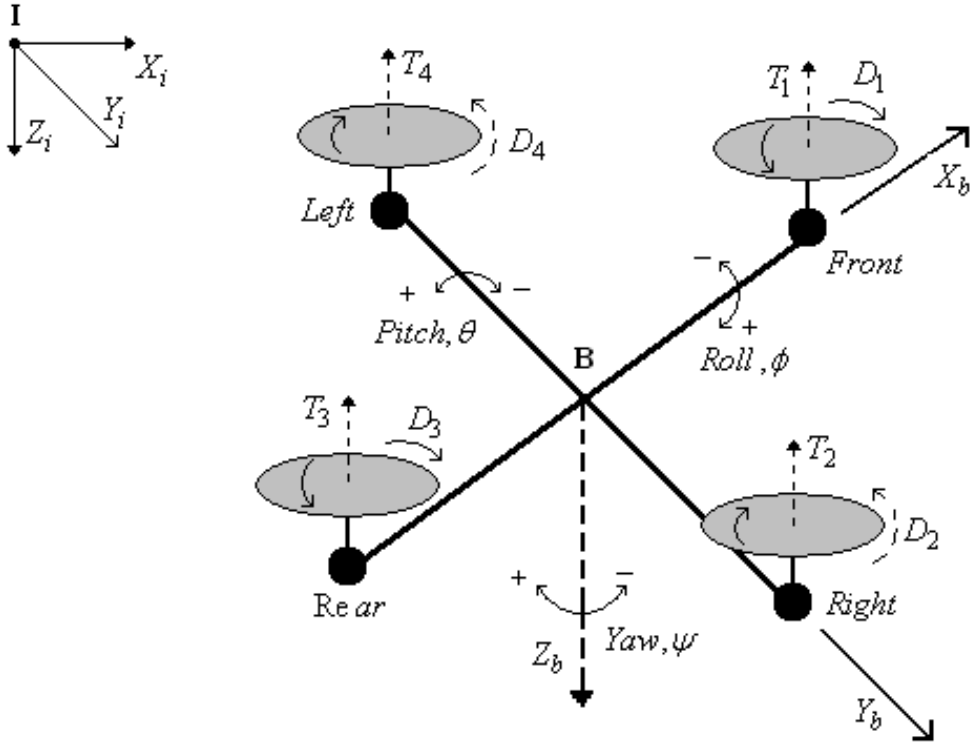
3. A QUADROTOR TÉRBELI MOZGÁSÁNAK DINAMIKUS MODELLJE [10, 11]

A Quadrotor sajátos aerodinamikai elrendezést jelent: a tartószerkezet végein elhelyezett villamos motorok közvetlenül hajtják a légcsavarokat, amelyek beállítási szöge nem változtatható. A motorok fordulatszáma egyenként is változtatható ebben az elrendezésben, így a négyrotoros légijármű helyből felszálló, VTOL[1]-képességekkel rendelkezik, valamint jó kormányozhatósági-, és irányíthatósági jellemzőkkel bír. A négyrotoros UAV dinamikus modelljét határozzuk meg az 1. ábra segítségével [10, 11]. Könnyen belátható, hogy az egyes tengelyeken elhelyezett motorok azonos irányban, vagy az óramutató járásával azonos, vagy azzal ellentétes irányban forognak, így az eredő reaktív nyomaték hatását sikerül kiküszöbölni.

„Függés” repülési helyzetben mind a négy motor fordulatszáma azonos, így a függőleges tengely mentén a manőverezést a négy motor fordulatszámának azonos mértékű, és azonos irányú megváltoztatásával tudjuk elérni. A bólintás, és a megfelelő oldalirányú mozgás létrehozására az 1, és a 3 motorok fordulatszámát ellentétes értelemben kell megváltoztatni. A bedöntési szög, és a megfelelő oldalirányú mozgás létrehozása a 2, és a 4 motorok

[1] VTOL: **V**ertical **T**ake-**o**ff and **L**anding

fordulatszámának ellentétes értelmű megváltoztatásával lehetséges. A legyező szög megváltoztatásához az egyes tengelyeken elhelyezett motorok fordulatszámának azonos, de a másik tengelyen elhelyezett motorokkal ellentétes értelmű megváltoztatása szükséges: így a reaktív nyomaték kiegyensúlyozatlansága miatt a quadrotor elfordul a függőleges tengely körül.



1. ábra. A négyrotoros UAV dinamikus viselkedése

Az 1. ábrán **I** jelöli az inercia(vonatkoztatási) rendszert, míg **B** jelöli a légijárműhöz rögzített „test” koordináta-rendszert. A légijármű „test” koordináta-rendszerben mért Euler-szögeinek változási sebessége az alábbi módon írható fel:

$$\begin{bmatrix} \dot{\phi} & \dot{\theta} & \dot{\psi} \end{bmatrix}^T = \mathbf{M}^{-1} \begin{bmatrix} \omega_{x_i} & \omega_{y_i} & \omega_{z_i} \end{bmatrix}^T = \mathbf{M}^{-1} \mathbf{A} \begin{bmatrix} \omega_{x_b} & \omega_{y_b} & \omega_{z_b} \end{bmatrix}^T, \tag{3.1}$$

ahol: ϕ bedöntési szög; θ bólintási szög; ψ irányszög; ω_{x_i} szögsebességek az inercia-rendszerben; ω_{x_b} szögsebességek a „test” koordináta rendszerben; valamint:

$$\mathbf{M} = \begin{bmatrix} \frac{c\psi}{c\theta} & \frac{s\psi}{c\theta} & 0 \\ -s\psi & c\psi & 0 \\ 0 & 0 & 1 \end{bmatrix}; \ \mathbf{A} = \begin{bmatrix} c\psi c\theta & c\psi s\theta s\phi - s\psi c\phi & c\psi s\theta c\phi - s\psi s\phi \\ s\psi c\theta & s\psi s\theta s\phi + c\psi c\phi & s\psi s\theta c\phi - c\psi s\phi \\ -s\theta & c\theta s\phi & c\theta c\phi \end{bmatrix} - \text{forgatómátrixok,}$$

ahol: c – cos, s – sin.

Tekintettel arra, hogy számunkra a későbbi feladatok megoldása miatt csak a „test” koordináta-rendszer **B** pontjának a sebessége a szabályozandó paraméter, ezért a „test” koordináta-rendszerben mért sebességeket az alábbi egyenlettel határozhatjuk meg [10, 11]:

$$\begin{bmatrix} \dot{x}_b & \dot{y}_b & \dot{z}_b \end{bmatrix}^T = \mathbf{A}^{-1} \begin{bmatrix} \dot{x}_i & \dot{y}_i & \dot{z}_i \end{bmatrix}^T, \tag{3.2}$$

ahol x_b, y_b, z_b koordináták a test-koordináta rendszerben, és x_i, y_i, z_i koordináták az inercia(referencia) koordináta rendszerben.

3.1. A quadrotor egyenesvonalú mozgásegyenletei

A mozgásegyenletek levezetése során feltételezzük, hogy

- a quadrotor szerkezete merev, és szimmetrikus;
- a quadrotor tömegközéppontja a **B** pontban helyezkedik el (l. 1. ábra);
- a légcsavar-lapátok merev szerkezetek, és a quadrotor nem végez bólintó mozgást.

Az *i*-edik légcsavarlapát által létesített felhajtóerő arányos az adott légcsavar forgási sebességének négyzetével, vagyis:

$$T_i = C_1\left(\frac{1-2\pi LCS}{P\alpha_i} + 2\pi\frac{\dot{z}_b - w_{z_b}}{P\alpha_i}\right), \tag{3.3}$$

ahol: $C_1 = k_t \rho A_p \alpha_i^2 R_p^2$; k_t aerodinamikai felhajtóerő tényező; ρ a levegő sűrűsége; A_p a légcsavar felülete; α_i az *i*-edik légcsavar szögsebessége; R_p a légcsavar sugara; L a légcsavar középpontjának távolsága az origótól; P a légcsavarlapátok beállítási szöge, és végül, w_{z_b} a légköri turbulencia vektorának *z*-tengelyre eső vetülete. C=1, ha i=1, vagy i=4. C= –1, ha i=2, vagy i=3. $S = \omega_{y_b}$, ha i=1, vagy i=3. $S = \omega_{x_b}$, ha i=2, vagy i=4.

A légijármű hossztengelye mentén ható erők eredője az alábbi egyenlettel írható le [10, 11]:

$$F_{wI} = \mathbf{A}\left[k_s(w_{x_b} - \dot{x}_b) \quad k_s(w_{y_b} - \dot{y}_b) \quad k_u(w_{z_b} - \dot{z}_b)\right]^T, \tag{3.4}$$

ahol: k_s, k_u az egyenesvonalú mozgás súrlódási együtthatói; w_{x_b} és w_{y_b} a légköri turbulencia vektorának *x–, és y*–tengelyekre eső vetületei, értelemszerűen.

A quadrotor térbeli lineáris mozgásának állapot–egyenlete a következő mátrixos alakban is megadható [10, 11]:

$$\begin{bmatrix}\ddot{x}_i\\ \ddot{y}_i\\ \ddot{z}_i\end{bmatrix} = -\begin{bmatrix}\omega_{x_b}\\ \omega_{y_b}\\ \omega_{z_b}\end{bmatrix} \times \begin{bmatrix}\dot{x}_i\\ \dot{y}_i\\ \dot{z}_i\end{bmatrix} + g\begin{bmatrix}0\\0\\1\end{bmatrix} + \frac{F_{wI}}{m} - \frac{T_1+T_2+T_3+T_4}{m}\mathbf{A}\begin{bmatrix}0\\0\\1\end{bmatrix}, \tag{3.5}$$

ahol: *g* a nehézségi gyorsulás, *m* a légijármű tömege.

3.2. A quadrotor forgómozgásának egyenletei

Ismeretes, hogy a légcsavarlapátok légellenállásból származó nyomatéka arányos a légcsavarlapát forgási sebességének a négyzetével, vagyis [10, 11]:

$$D_i = C_2\left(\frac{1-2\pi LCS}{P\alpha_i} + 2\pi\frac{\dot{z}_b - w_{z_b}}{P\alpha_i}\right), \tag{3.6}$$

ahol: $C_2 = k_d \rho A_p \alpha_i^2 R_p^3$; k_d a nyomatéki együttható.

A légcsavarlapátok eredő reakciónyomatéka az alábbi egyenlettel írható le:

$$I_{ct} = J_p\left(-\dot{\alpha}_1 + \dot{\alpha}_2 - \dot{\alpha}_3 + \dot{\alpha}_4\right), \tag{3.7}$$

ahol: J_p egy légcsavarlapát tehetetlenségi nyomatéka.

A súrlódási terhelő nyomatékot az alábbi egyenlet alapján is számíthatjuk:

$$\mathbf{M}_f = k_r\begin{bmatrix}\dot{\phi} & \dot{\theta} & \dot{\psi}\end{bmatrix}^T, \tag{3.8}$$

ahol: k_r a súrlódási együttható.

A légijármű motorjának forgórészére redukált nemirányítható zavarások (pl. légköri turbulencia) a következő összefüggéssel írható le:

$$\tau_d = \begin{bmatrix}\tau_{x_b} & \tau_{y_b} & \tau_{z_b}\end{bmatrix}^T, \tag{3.9}$$

A légijármű giroszkópikus nyomatéka a következő egyenlettel írható le:

$$\mathbf{M}_g = J_p\begin{bmatrix}\dot{\theta}\alpha & \dot{\phi}\alpha & 0\end{bmatrix}^T, \tag{3.10}$$

ahol: $\alpha = -\alpha_1 + \alpha_2 - \alpha_3 + \alpha_4$.

Mindezek alapján, a quadrotor térbeli forgómozgásának állapot–egyenlete a következő mátrixos alakban is megadható [10, 11]:

$$\begin{bmatrix}\dot{\omega}_{x_b}\\ \dot{\omega}_{y_b}\\ \dot{\omega}_{z_b}\end{bmatrix} = -J^{-1}\omega \times J\begin{bmatrix}\omega_{x_b}\\ \omega_{y_b}\\ \omega_{z_b}\end{bmatrix} - J^{-1}\left(\mathbf{M}_f + \tau_d + \mathbf{M}_g\right) + J^{-1}\begin{bmatrix}L(T_4 - T_2)\\ L(T_1 - T_3)\\ D_1 - D_2 + D_3 - D_4 + I_{ct}\end{bmatrix}, \tag{3.11}$$

ahol: $\omega = \begin{bmatrix}0 & -\omega_{z_b} & \omega_{y_b}\\ \omega_{z_b} & 0 & -\omega_{x_b}\\ -\omega_{y_b} & \omega_{x_b} & 0\end{bmatrix}$, $J = \begin{bmatrix}J_{xx} & 0 & 0\\ 0 & J_{yy} & 0\\ 0 & 0 & J_{zz}\end{bmatrix}$ a főtehetetlenségi mátrix; J_{xx}, J_{yy}, J_{zz} a hossz-, a kereszt-, és a függőleges tengelyre vett főtehetetlenségi nyomatékok, értelemszerűen.

3.3. A quadrotor egyenáramú motorjának dinamikája

Ismeretes, hogy az egyenáramú motor – kis értékű motor induktivitások esetén – dinamikus egyenlete a következő alakban írható fel:

$$J_p\dot{\alpha}_i = G\tau_{m_i} - D_i, \tag{3.12}$$

ahol: $\tau_{m_i} = \left(k_i(V_i - \frac{k_v\alpha_i}{G})R^{-1}\right)$ a motor dinamikus gyorsító nyomatéka; k_i a motor állandója; k_v a motor forgási sebesség állandója; V_i a motor vezérlő feszültsége; R a motorellenállás; G a „motor-légcsavar” rendszer áttételi száma.

Vizsgáljuk kismagasságú függés repülési helyzetben a quadrotor dinamikáját, ha a függőleges tengely mentén kell emelkedő mozgást végrehajtania. A kiindulási feltételek – zavarásmentes esetre – most az alábbiak lesznek:

$$\theta = 0^o; \phi = 0^o; \psi = 0^o; v_{x_{b_o}} = 0m/s; v_{y_{b_o}} = 0m/s; v_{z_{b_o}} = 0m/s\,, \tag{3.13}$$

A (3.1)–(3.5) egyenleteket felhasználva, a (3.13) kezdeti feltételek figyelembe vételével a quadrotor függőleges tengely mentén végrehajtott mozgásának dinamikus egyenlete az alábbi alakban írható fel:

$$\ddot{z}_b = \frac{F_{mI}}{m} - \frac{T_1 + T_2 + T_3 + T_4}{m} + g\,, \tag{3.14}$$

vagy más alakban:

$$\ddot{z}_b + \frac{\dot{z}_b}{m} = g - \frac{T_1 + T_2 + T_3 + T_4}{m} = g - \frac{4T}{m}\,, \tag{3.15}$$

Az egyes rotorlapátok felhajtóereje az alábbi egyenlettel adható meg:

$$T = C_1\left(\frac{1}{P\alpha_i} + 2\pi\frac{\dot{z}_b}{P\alpha_i}\right), \tag{3.16}$$

ahol: $C_1 = k_t \rho A_p\, \alpha_i^2 R_p^2 = 4{,}15872 \cdot 10^{-6}\, \alpha_i^2$.

Helyettesítsük be a (3.16) egyenletet a (3.15) egyenletbe:

$$\ddot{z}_b + \frac{\dot{z}_b}{m} = g - \frac{4T}{m} = g - \frac{4}{m}C_1\left(\frac{1}{P\alpha_i} + 2\pi\frac{\dot{z}_b}{P\alpha_i}\right), \tag{3.17}$$

és rendezzük a kapott egyenletet:

$$\ddot{z}_b + \frac{\dot{z}_b}{m} + \frac{4}{m}C_1 2\pi\frac{\dot{z}_b}{P\alpha_i} = g - \frac{4}{m}C_1\frac{1}{P\alpha_i}\,, \tag{3.18}$$

valamint további rendezéssel a következő összefüggésre jutunk:

$$\ddot{z}_b + \dot{z}_b\left(\frac{1}{m} + \frac{4}{m}C_1 2\pi\frac{1}{P\alpha_i}\right) = g - \frac{4}{m}C_1\frac{1}{P\alpha_i}\,. \tag{3.19}$$

Egy hipotetikus quadrotor paramétereinek felhasználásával a (3.19) egyenlet a következő alakban írható fel [10, 11]:

$$\ddot{z}_b + \dot{z}_b\left(0{,}222568 + 153{,}0451369 \cdot 10^{-6}\alpha_i\right) = 9{,}81 - 24{,}35789 \cdot 10^{-6}\alpha_i\,. \tag{3.20}$$

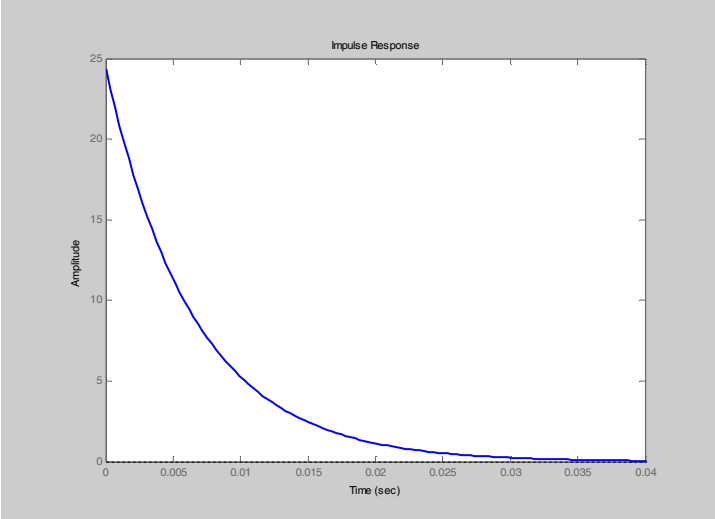
Legyen $\alpha_{i_o} = 1000\, ford/p$. Akkor a függőleges sebesség változását az alábbi egyenlet adja meg:

$$\dot{v}_b + v_b 153{,}2677049 = 9{,}81 - 24{,}35789\Delta\alpha_i\,. \tag{3.21}$$

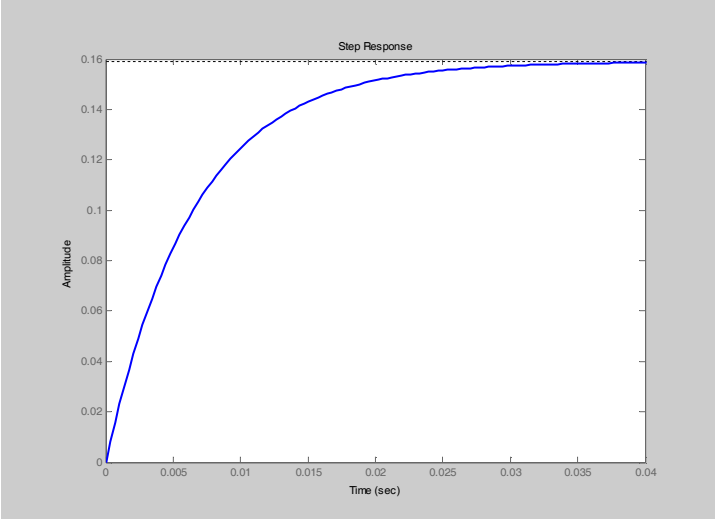
A (3.21) egyenlet alapján a quadrotor átviteli függvénye a következő lesz:

$$Y(s) = \frac{v_b(s)}{\Delta\alpha_i(s)} = -\frac{24{,}35789}{153{,}2677049 + s}. \tag{3.22}$$

A továbbiakban vizsgáljuk meg a quadrotor viselkedését idő-, és frekvenciatartományban. A számítógépes szimuláció eredménye a 2. ábrán látható. A 2. ábra alapján megállapíthatjuk, hogy a quadrotor gyorsan reagál a bemenetekre, képes nagy sebességgel reagálni a gerjesztő jelre, és állandó sebességgel emelkedni (2.b. ábra). A súlyfüggvény állandósult állapotban zérushoz tart, így az irányított quadrotor stabilis viselkedésű.



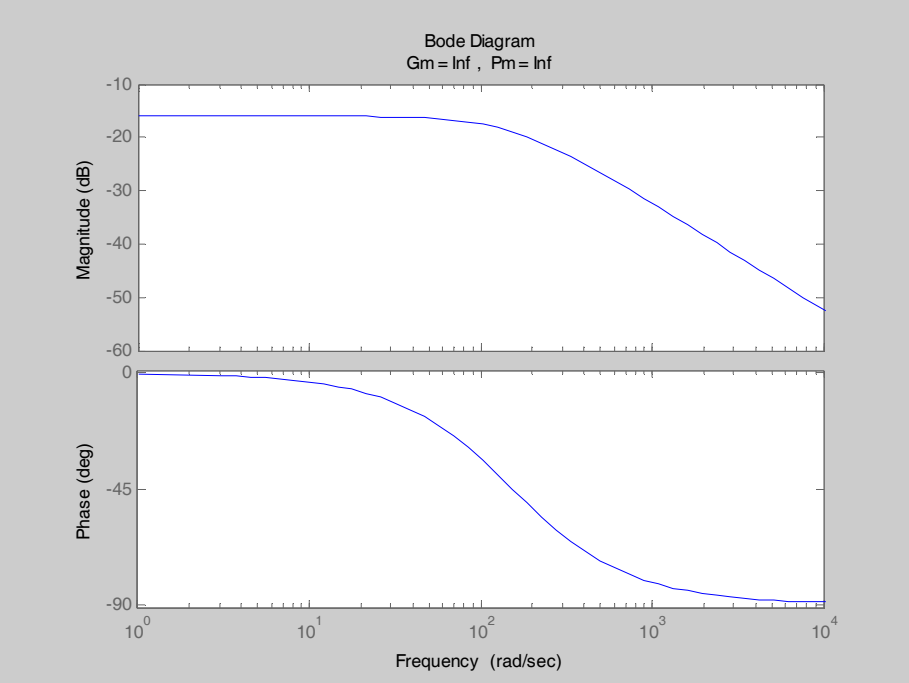
a) Súlyfüggvény



b) Átmeneti függvény

2. ábra Számítógépes analízis eredménye.

A 3. ábrán a quadrotor frekvenciatartománybeli viselkedése látható. A 3. ábrán jól látható, hogy a quadrotor alul-áteresztő jelleggel viselkedik, nagyfrekvenciás tartományban „levágja” a bemeneti jeleket, jól szűri a nagyfrekvenciás zajokat. Úgy az erősítési-, mint a fázistartalék végtelen értékű.



3. ábra. Viselkedés frekvenciatartományban – Bode diagram.

4. LQ-ALAPÚ SZABÁLYOZÓTERVEZÉS QUADROTOR FÜGGŐLEGES TÉRBELI MOZGÁSÁNAK AUTOMATIZÁLÁSA

Lineáris, autonóm szabályozási rendszer állapot-, és a kimeneti egyenletet az alábbi alakban szokás megadni [1, 2, 10, 11]:

$$\dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u}\,;\, \mathbf{y} = \mathbf{C}\mathbf{x} + \mathbf{D}\mathbf{u}\,, \tag{4.1}$$

ahol: **x** állapotvektor, **u** bemeneti vektor, **y** kimeneti vektor, **A** állapotmátrix, **B** bemeneti mátrix, **C** kimeneti mátrix és **D** segédmátrix.

Többváltozós állandó paraméterű irányított rendszer esetében a minimálandó funkcionált az alábbi egyenlettel szokás megadni [1, 2]:

$$J = \frac{1}{2}\int_0^{\infty}\left(\mathbf{x}^{\mathrm{T}}\mathbf{Q}\,\mathbf{x} + \mathbf{u}^{\mathrm{T}}\mathbf{R}\,\mathbf{u}\right)dt \rightarrow \mathrm{M}in\,, \tag{4.2}$$

ahol: **Q** pozitív definit (vagy pozitív szemidefinit) diagonális súlyozó mátrix, **R** pozitív definit diagonális súlyozó mátrix. A szabályozótervezés során a súlyozó mátrixok beállítására az ún. azonos(egységnyi) súlyozás elvét, vagy a reciprok négyzetes szabályt is alkalmazhatjuk, majd a mátrixok finomhangolását hajtjuk végre.

Ha a **Q** felülsúlyozott az **R** mátrixhoz képest, akkor a zárt szabályozási rendszer minőségi jellemzői változnak lényeges mértékben. Ha az **R** mátrix túlsúlyozott a **Q** mátrix elemeihez képest, akkor a szabályozás nagy energiaigényű lesz [1, 2, 10, 11]. Az integrálandó $\mathbf{x}^{\mathrm{T}}\mathbf{Q}\,\mathbf{x}$ kvadratikus alak a minőségi jellemzőkről hordoz információt, míg az $\mathbf{u}^{\mathrm{T}}\mathbf{R}\,\mathbf{u}$ kvadratikus alak a költségeket jellemzi.

Ezek a tagok skalár mennyiségek, mivel:

$$\mathbf{x}^{\mathrm{T}}\mathbf{Q}\,\mathbf{x}=\begin{bmatrix}x_1 & . & . & . & x_n\end{bmatrix}\begin{bmatrix}q_1 & 0 & . & 0 & 0\\ 0 & q_2 & . & . & 0\\ . & . & . & . & .\\ 0 & . & . & q_{n-1} & 0\\ 0 & 0 & . & 0 & q_n\end{bmatrix}\begin{bmatrix}x_1\\ .\\ .\\ .\\ x_n\end{bmatrix}=\begin{bmatrix}x_1 & . & . & . & x_n\end{bmatrix}\begin{bmatrix}q_1 x_1\\ .\\ .\\ .\\ q_n x_n\end{bmatrix}=\sum_{i=1}^{n} q_i\, x_i^2(t), \quad (4.3)$$

valamint

$$\mathbf{u}^{\mathrm{T}}\mathbf{R}\,\mathbf{u}=\begin{bmatrix}u_1 & . & . & . & u_n\end{bmatrix}\begin{bmatrix}r_1 & 0 & . & 0 & 0\\ 0 & r_2 & . & . & 0\\ . & . & . & . & .\\ 0 & . & . & r_{n-1} & 0\\ 0 & 0 & . & 0 & r_n\end{bmatrix}\begin{bmatrix}u_1\\ .\\ .\\ .\\ u_n\end{bmatrix}=\begin{bmatrix}u_1 & . & . & . & u_n\end{bmatrix}\begin{bmatrix}r_1 u_1\\ .\\ .\\ .\\ r_n u_n\end{bmatrix}=\sum_{j=1}^{n} r_j\, u_j^2(t), \quad (4.4)$$

A (4.3) és a (4.4) egyenletek alapján azt mondhatjuk, hogy a (4.2) integrálkritérium az $x_i^2(t)$ és az $u_j^2(t)$ görbék alatti területet minimálja.

4.1. Az elfajult Ricatti-féle mátrixegyenlet

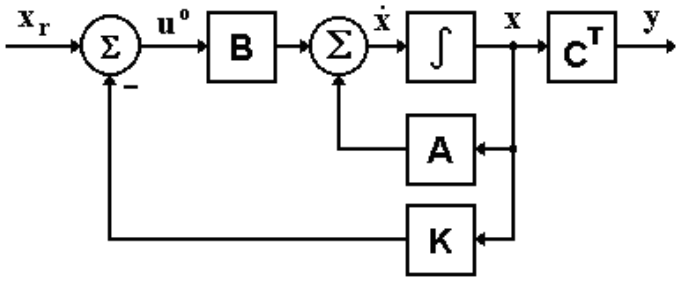
Tekintsük adottnak a vizsgált rendszer állapotegyenletét [1, 2]:

$$\dot{\mathbf{x}} = \mathbf{A}\,\mathbf{x} + \mathbf{B}\,\mathbf{u}. \quad (4.5)$$

Az optimális vezérlési törvény [1, 2, 10, 11]:

$$\mathbf{u}^{\mathbf{o}}(\mathrm{t}) = -\,\mathbf{K}\,\mathbf{x}(\mathrm{t}) \quad (4.6)$$

alakú, amely biztosítja a (4.2) négyzetes integrálkritérium minimális értékét. Az optimálási feladat megoldottnak tekinthető bármely $\mathbf{x}(0)$ kezdeti értékre, ha ismertek a $\mathbf{K}$ mátrix elemei. Az optimális szabályozási rendszer hatásvázlata a 4. ábrán látható. A referencia jel legyen zérusértékű, vagyis, $x_r(t)=0$.



4. ábra. A teljes állapot-visszacsatolású rendszer hatásvázlata.

Helyettesítsük a (4.6) egyenletet a (4.5) állapotegyenletbe. A következő egyenletet kapjuk:

$$\dot{\mathbf{x}} = \mathbf{A}\,\mathbf{x} - \mathbf{B}\,\mathbf{K}\,\mathbf{x} = (\mathbf{A} - \mathbf{B}\,\mathbf{K})\,\mathbf{x}. \quad (4.7)$$

A továbbiakban feltételezzük, hogy az $(\mathbf{A}-\mathbf{B}\,\mathbf{K})$ mátrix sajátértékei negatív valós részűek. Helyettesítsük a (4.7) egyenletet a (4.2) egyenletbe:

$$\mathrm{J}=\frac{1}{2}\int_0^{\infty}(\mathbf{x}^{\mathrm{T}}\mathbf{Q}\mathbf{x}+\mathbf{x}^{\mathrm{T}}\mathbf{K}^{\mathrm{T}}\mathbf{R}\mathbf{K}\mathbf{x})\,\mathrm{dt}=\frac{1}{2}\int_0^{\infty}\mathbf{x}^{\mathrm{T}}(\mathbf{Q}+\mathbf{K}^{\mathrm{T}}\mathbf{R}\mathbf{K})\mathbf{x}\,\mathrm{dt}\rightarrow\mathrm{Min}. \quad (4.8)$$

A (4.2) integrálkritérium minimálásához Ljapunov második, közvetlen módszerét használjuk. Feltételezzük, hogy bármely **x** állapotvektorhoz rendelhető egy valós elemű **P** pozitív definit Hermite-mátrix, amelyre igaz, hogy $\mathbf{P} = \mathbf{P}^{\mathbf{T}}$. Ebben az esetben igaz, hogy:

$$\mathbf{x}^{\mathbf{T}}(\mathbf{Q}+\mathbf{K}^{\mathbf{T}}\mathbf{R}\mathbf{K})\mathbf{x} = -\frac{\mathrm{d}}{\mathrm{dt}}(\mathbf{x}^{\mathbf{T}}\mathbf{P}\mathbf{x}). \tag{4.9}$$

Az $\mathbf{x}^{\mathbf{T}}\mathbf{P}\ \mathbf{x}$ kvadratikus alak deriválása és a (4.9) egyenlet felhasználása után kapjuk, hogy:

$$\mathbf{x}^{\mathbf{T}}(\mathbf{Q}+\mathbf{K}^{\mathbf{T}}\mathbf{R}\mathbf{K})\mathbf{x} = -\mathbf{x}^{\mathbf{T}}\mathbf{P}\mathbf{x} - \mathbf{x}^{\mathbf{T}}\mathbf{P}\mathbf{x} = -\mathbf{x}^{\mathbf{T}}\left[(\mathbf{A}-\mathbf{B}\mathbf{K})^{\mathbf{T}}\mathbf{P}+\mathbf{P}(\mathbf{A}-\mathbf{B}\mathbf{K})\right]\mathbf{x}. \tag{4.10}$$

Ljapunov második közvetlen módszere szerint, ha az $(\mathbf{A}-\mathbf{B}\mathbf{K})$ mátrix sajátértékei negatív valós részűek, akkor $\mathbf{Q}+\mathbf{K}^{\mathbf{T}}\mathbf{R}\mathbf{K}$ pozitív definit mátrix esetén létezik olyan pozitív definit **P** mátrix, amelyre igaz, hogy:

$$(\mathbf{A}-\mathbf{B}\mathbf{K})^{\mathbf{T}}\mathbf{P}+\mathbf{P}(\mathbf{A}-\mathbf{B}\mathbf{K}) = -(\mathbf{Q}+\mathbf{K}^{\mathbf{T}}\mathbf{R}\mathbf{K}). \tag{4.11}$$

A (4.11) egyenletet szokás Ljapunov-féle mátrix egyenletnek nevezni. A négyzetes integrálkritérium most a következő alakban adható meg:

$$\mathrm{J} = \frac{\mathbf{1}}{\mathbf{2}}\int_{\mathbf{0}}^{\infty}\mathbf{x}^{\mathbf{T}}(\mathbf{Q}+\mathbf{K}^{\mathbf{T}}\mathbf{R}\mathbf{K})\mathbf{x}\,\mathrm{dt} = -\left[\mathbf{x}^{\mathbf{T}}\mathbf{P}\mathbf{x}\right]_{\mathbf{0}}^{\infty} = -\mathbf{x}^{\mathbf{T}}(\infty)\mathbf{P}\mathbf{x}(\infty)+\mathbf{x}^{\mathbf{T}}(0)\mathbf{P}\mathbf{x}(0). \tag{4.12}$$

Mivel az $\mathbf{A}-\mathbf{B}\mathbf{K}$ mátrix sajátértékei negatív valós részűek, ezért $\mathbf{x}(\infty)\to 0$. A (4.12) egyenlet a következő alakban írható fel:

$$\mathrm{J} = \mathbf{x}^{\mathbf{T}}(0)\mathbf{P}\mathbf{x}(0). \tag{4.13}$$

Mint az a (4.13) egyenletből látszik, a (4.12) integrálkritérium függ az **x**(0) kezdeti feltételtől is. Korábbról ismeretes, hogy az **R** mátrix valós elemű pozitív definit Hermite-féle hermetikus mátrix, ezért igaz, hogy:

$$\mathbf{R} = \mathbf{T}^{\mathbf{T}}\mathbf{T}. \tag{4.14}$$

ahol **T** nemszinguláris (reguláris) mátrix.

A (4.14) egyenlet figyelembevételével a (4.11) egyenletet a következő módon írhatjuk fel :

$$(\mathbf{A}^{\mathbf{T}}-\mathbf{K}^{\mathbf{T}}\mathbf{B}^{\mathbf{T}})\mathbf{P}+\mathbf{P}(\mathbf{A}-\mathbf{B}\mathbf{K})+\mathbf{Q}+\mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}\mathbf{T}\mathbf{K} = 0. \tag{4.15}$$

Elvégezve a (4.15) egyenlet kijelölt műveleteit, kapjuk, hogy:

$$\mathbf{A}^{\mathbf{T}}\mathbf{P}+\mathbf{P}\mathbf{A}+\left(-\mathbf{K}^{\mathbf{T}}\mathbf{B}^{\mathbf{T}}\mathbf{P}-\mathbf{P}\mathbf{B}\mathbf{K}+\mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}\mathbf{T}\mathbf{K}\right)+\mathbf{Q}=0. \tag{4.16}$$

Felhasználva, hogy $\mathbf{P}=\mathbf{P}^{\mathbf{T}}$, valamint $\mathbf{R}^{-1}=\mathbf{T}^{-1}(\mathbf{T}^{\mathbf{T}})^{-1}$, a zárójelben álló kifejezés tovább alakítható:

$$\mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}\mathbf{T}\mathbf{K}-\mathbf{K}^{\mathbf{T}}\mathbf{B}^{\mathbf{T}}\mathbf{P}-\mathbf{P}\mathbf{B}\mathbf{K} = \mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}\mathbf{T}\mathbf{K}-\mathbf{K}^{\mathbf{T}}\left[\mathbf{T}^{\mathbf{T}}\left(\mathbf{T}^{\mathbf{T}}\right)^{-1}\right]\mathbf{B}^{\mathbf{T}}\mathbf{P}-\mathbf{P}^{\mathbf{T}}\mathbf{B}\mathbf{K}+\left(\mathbf{P}^{\mathbf{T}}-\mathbf{P}\right)\mathbf{B}\mathbf{R}^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P} =$$

$$= \mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}\mathbf{T}\mathbf{K}-\mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}\left(\mathbf{T}^{\mathbf{T}}\right)^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P}-\mathbf{P}^{\mathbf{T}}\mathbf{B}\left(\mathbf{T}^{-1}\mathbf{T}\right)\mathbf{K}+\mathbf{P}^{\mathbf{T}}\mathbf{B}\left[\mathbf{T}^{-1}\left(\mathbf{T}^{\mathbf{T}}\right)^{-1}\right]\mathbf{B}^{\mathbf{T}}\mathbf{P}-\mathbf{P}\mathbf{B}\mathbf{R}^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P} =$$

$$= \left[\mathbf{K}^{\mathbf{T}}\mathbf{T}^{\mathbf{T}}-\mathbf{P}^{\mathbf{T}}\mathbf{B}\mathbf{T}^{-1}\right]\left[\mathbf{T}\mathbf{K}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]-\mathbf{P}\mathbf{B}\mathbf{R}^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P} = \tag{4.17}$$

$$= \left[\mathbf{T}\mathbf{K}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]^{\mathbf{T}}\left[\mathbf{T}\mathbf{K}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]-\mathbf{P}\mathbf{B}\mathbf{R}^{-1}\mathbf{B}^{\mathbf{T}}\mathbf{P}$$

A (4.16) egyenlet most az alábbi alakban írható fel:

$$\mathbf{A}^{\mathbf{T}}\mathbf{P}+\mathbf{PA}+\left[\mathbf{TK}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]^{\mathbf{T}}\left[\mathbf{TK}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]-\mathbf{PBR}^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}+\mathbf{Q}=0\,. \qquad (4.18)$$

A négyzetes integrálkritérium minimálása, vagyis az optimális vezérlési törvény **K** teljes állapot-visszacsatolási mátrixának meghatározása gyakorlatilag az

$$\mathbf{x}^{\mathbf{T}}\left[\mathbf{TK}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]^{\mathbf{T}}\left[\mathbf{TK}-\left(\mathbf{T}^{\mathbf{T}}\right)^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\right]\mathbf{x} \qquad (4.19)$$

szorzat minimálását jelenti. Mivel a (4.19) mátrix nem negatív, ezért a (4.18) egyenlet minimális értéket akkor vesz fel, ha

$$\mathbf{TK}=\left(\mathbf{T}^{\mathbf{T}}\right)^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\,. \qquad (4.20)$$

A (4.20) egyenletből most fejezzük ki a **K** állapot-visszacsatolási mátrixot:

$$\mathbf{K}^{\mathbf{o}}=\mathbf{T}^{-\mathbf{1}}\left(\mathbf{T}^{\mathbf{T}}\right)^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}=\mathbf{R}^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\,. \qquad (4.21)$$

A (4.21) egyenlet definiálja az optimális **K** visszacsatolási mátrixot. Az optimális vezérlési törvény ily módon a következő lesz:

$$\mathbf{u}^{\mathbf{o}}(t)=-\mathbf{K}^{\mathbf{o}}\mathbf{x}(\mathrm{t})=-\mathbf{R}^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}\mathbf{x}(\mathrm{t})\,. \qquad (4.22)$$

A **P** költségmátrix megállapítására gyakran alkalmazzák az ún. elfajult Ricatti algebrai mátrixegyenletet:

$$\mathbf{A}^{\mathbf{T}}\mathbf{P}+\mathbf{PA}-\mathbf{PBR}^{-\mathbf{1}}\mathbf{B}^{\mathbf{T}}\mathbf{P}+\mathbf{Q}=0\,. \qquad (4.23)$$

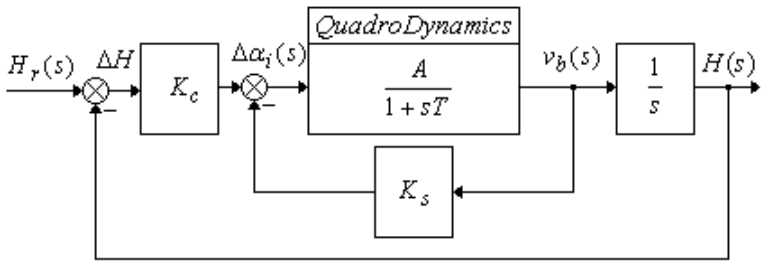
Az eddig elhangzottak alapján megfogalmazhatjuk az LQR optimálási feladat megoldásának lépéseit:

1, A (4.23) egyenlet alapján meghatározzák a **P** pozitív definit költség (Ljapunov) mátrixot;

2, A kapott **P** mátrixot behelyettesítik a (4.22) egyenletbe. A **K** visszacsatolási mátrix optimális, az optimális vezérlési törvényt a (4.22) egyenlet definiálja.

4.2 Quadrotor magasságstabilizáló rendszere szabályozójának előzetes tervezése

A quadrotor magasságstabilizáló rendszere az 5. ábrán látható.



5. ábra. A magasságstabilizáló rendszer hatásvázlata.

Az 5. ábra alapján írjuk fel a szabályozási rendszer állapot-egyenletét [10, 11]:

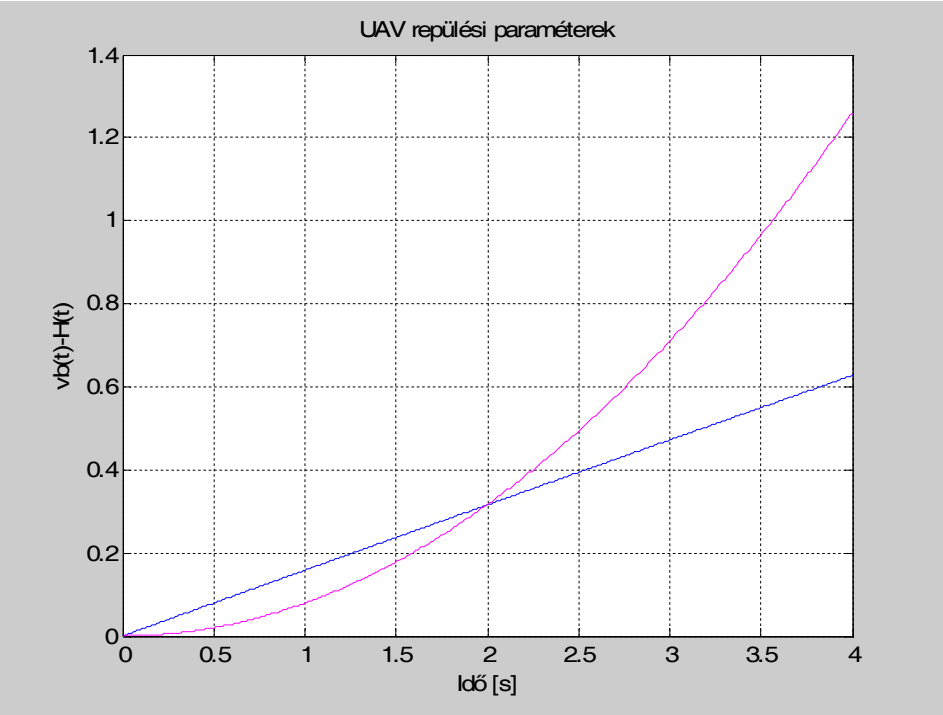
$$v_b(s)=\frac{A}{1+sT}\Delta\alpha_i(s)\;\rightarrow\;\dot{v}_b(t)=-\frac{v_b(t)}{T}+\frac{A}{T}\Delta\alpha_i(t) \qquad (4.24)$$

$$H(s)=\frac{1}{s}v_b(s)\;\rightarrow\;\dot{H}(t)=v_b(t) \qquad (4.25)$$

A (4.24), és a (4.25) egyenletek alapján a rendszer állapotegyenlete a következő mátrixos alakban írható fel:

$$\dot{\mathbf{x}}(t)=\begin{bmatrix}\dot{v}_b(t)\\ \dot{H}(t)\end{bmatrix}=\begin{bmatrix}-\frac{1}{T} & 0\\ 1 & 0\end{bmatrix}\begin{bmatrix}v_b(t)\\ H(t)\end{bmatrix}+\begin{bmatrix}A/T\\ 0\end{bmatrix}\Delta\alpha_i(t) \tag{4.26}$$

A nemirányított quadrotor átmeneti függvénye a 6. ábrán látható.



6. ábra. Nemirányított UAV átmeneti függvények

Függőleges repülési sebesség Repülési magasság

A zárt szabályozási rendszer vezérlési törvénye az alábbi egyenlettel adható meg:

$$\mathbf{u}(t)=\Delta\alpha_i(t)=-H(t)K_c-v_b(t)K_s=-\mathbf{K}\mathbf{x}\,, \tag{4.27}$$

ahol: $\mathbf{x}=\begin{bmatrix}v_b & H\end{bmatrix}^T$ - állapot-vektor; $\mathbf{K}=\begin{bmatrix}K_c & K_s\end{bmatrix}$ - teljes állapot-visszacsatolási mátrix.

Tervezzük meg az optimális állapot-visszacsatolási mátrixot az alábbi, un. egységnyi, azonos súlyozás elvén meghatározott súlyozó mátrixok esetén [1, 2, 10, 11]:

$$\mathbf{Q}_1=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix};r_1=1\,. \tag{4.28}$$

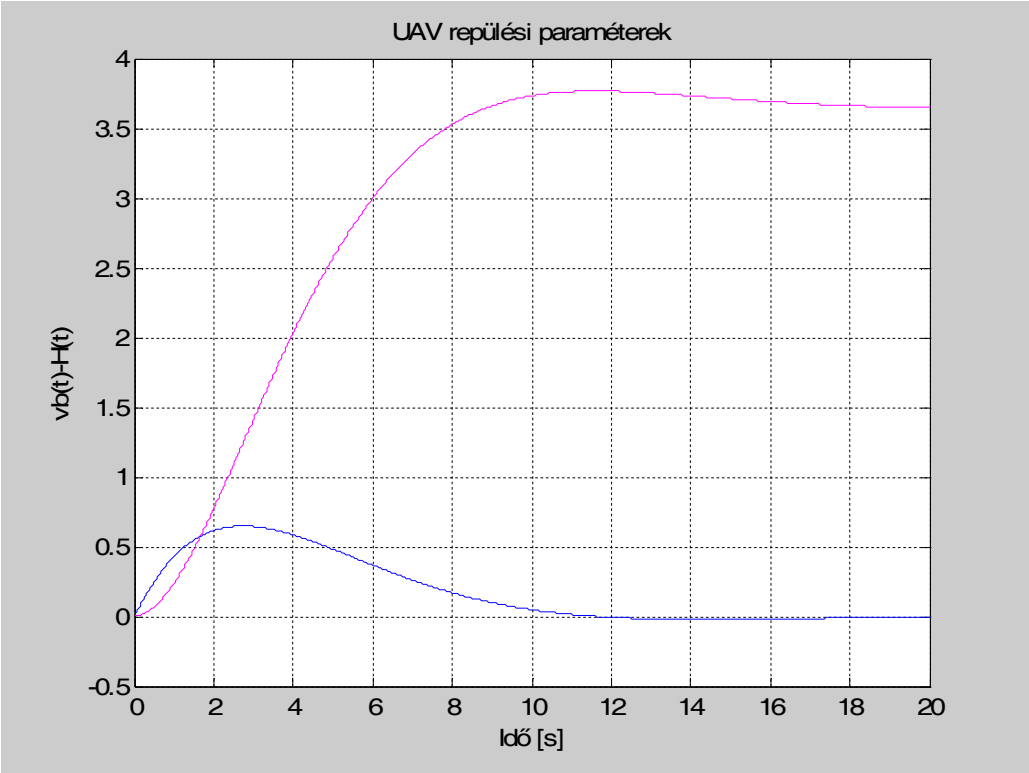
A teljes állapot-visszacsatolási mátrix most a következő lesz [10, 11]:

$$\mathbf{K}_1=\begin{bmatrix}K_c & K_s\end{bmatrix}=\begin{bmatrix}3{,}6449 & 1\end{bmatrix}, \tag{4.29}$$

A zárt szabályozási rendszer átmeneti függvénye a $H_r(t)=1(t)$ bemeneti jelre az (5.28) súlyozás esetén a 7. ábrán látható.

A 7. ábrán jól látható, hogy az egységnyi bemeneti jelre adott válasz stacioner értéke $H(\infty)\approx 3{,}7m$, tehát az ideális alapjel követés nem valósul meg [10, 11]. A zárt szabályozási rendszer minőségi jellemzői nem felelnek meg az előírt értékeknek [12], bár meg kell jegyezni, hogy a hivatkozott katonai szabvány az ember vezette légijárművekre vonatkozik, így annak alkalmazása az UAV-kra túlságosan szigorú minőségi követelménynek tűnik.

Megemlítjük, hogy a pilóta nélküli repülőgépekre a mai napig minőségi követelményrendszer nem áll rendelkezésre.



7. ábra. UAV zárt szabályozási rendszer átmeneti függvényei
Függőleges repülési sebesség Repülési magasság

A zárt szabályozási rendszer minőségi jellemzői az alábbiak lesznek:

Sajátértékek	Csillapítási tényező, ξ	Körfrekvencia, [rad/s]
$-0{,}293 \pm 0{,}27i$	0,735	0,399

Hangoljuk a (4.28) súlyozó mátrixokat heurisztikusan. Számos kísérleti beállítás, és próba után, a zárt szabályozási rendszer előírt minőségi jellemzőit teljesítő súlyozó mátrix-kombináció a következő lesz [1, 2, 10,11]:

$$\mathbf{Q}_2 = \begin{bmatrix} 0{,}97 & 0 \\ 0 & 1 \end{bmatrix}; r_2 = 0{,}000005\,. \tag{4.30}$$

A (4.30) súlyozó mátrixok alapján határozzuk meg a teljes állapot-visszacsatolási mátrixot:

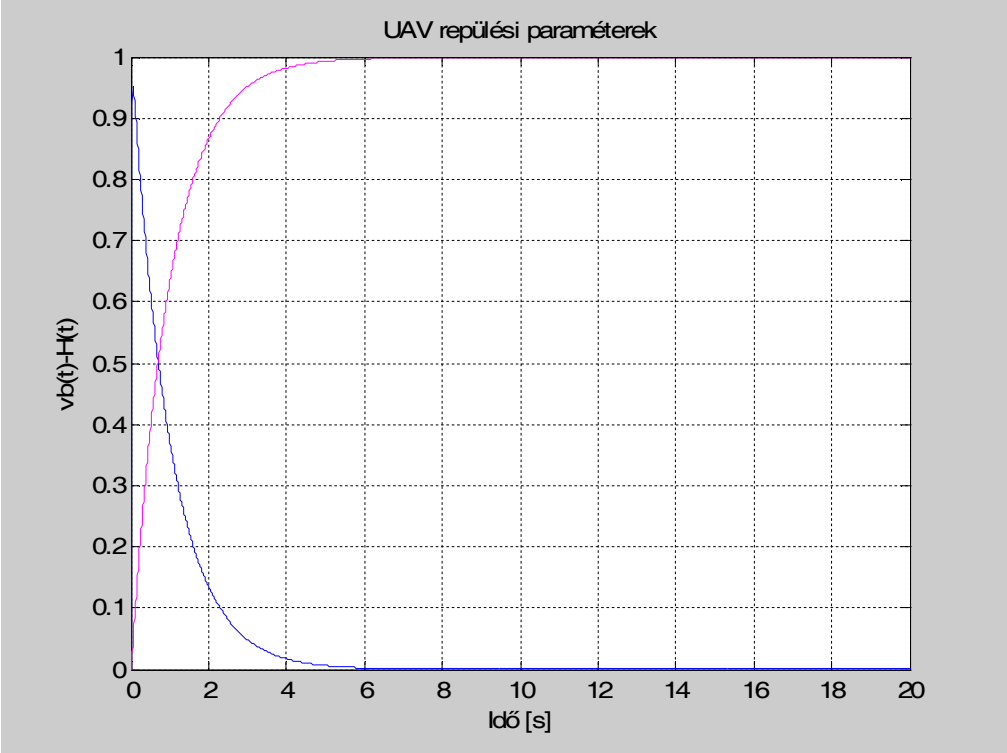
$$\mathbf{K}_2 = \begin{bmatrix} K_c & K_s \end{bmatrix} = \begin{bmatrix} 446{,}7565 & 447{,}2136 \end{bmatrix}, \tag{4.31}$$

A zárt szabályozási rendszer átmeneti függvénye a $H_r(t) = 1(t)$ bemeneti jelre az (5.30) súlyozó mátrixok esetére a 8. ábrán látható.

A 8. ábrán jól látható, hogy az egységnyi bemeneti jelre adott válasz stacioner értéke $H(\infty) = 1m$, tehát megvalósul az ideális alapjel követés. A zárt szabályozási rendszer minőségi jellemzői megfelelnek meg az előírt értékeknek [12].

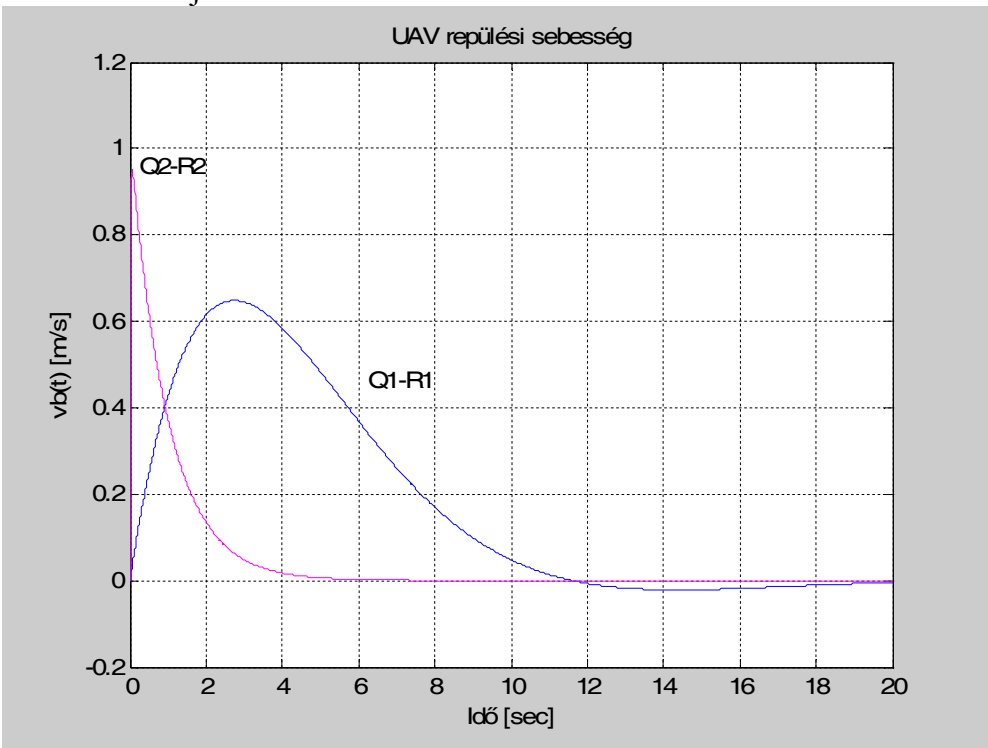
A módosított (hangolt) zárt szabályozási rendszer minőségi jellemzői az alábbiak lesznek:

Sajátértékek	Csillapítási tényező, ξ	Körfrekvencia, [rad/s]
-70	1	70
$-1{,}02$	1	1,02

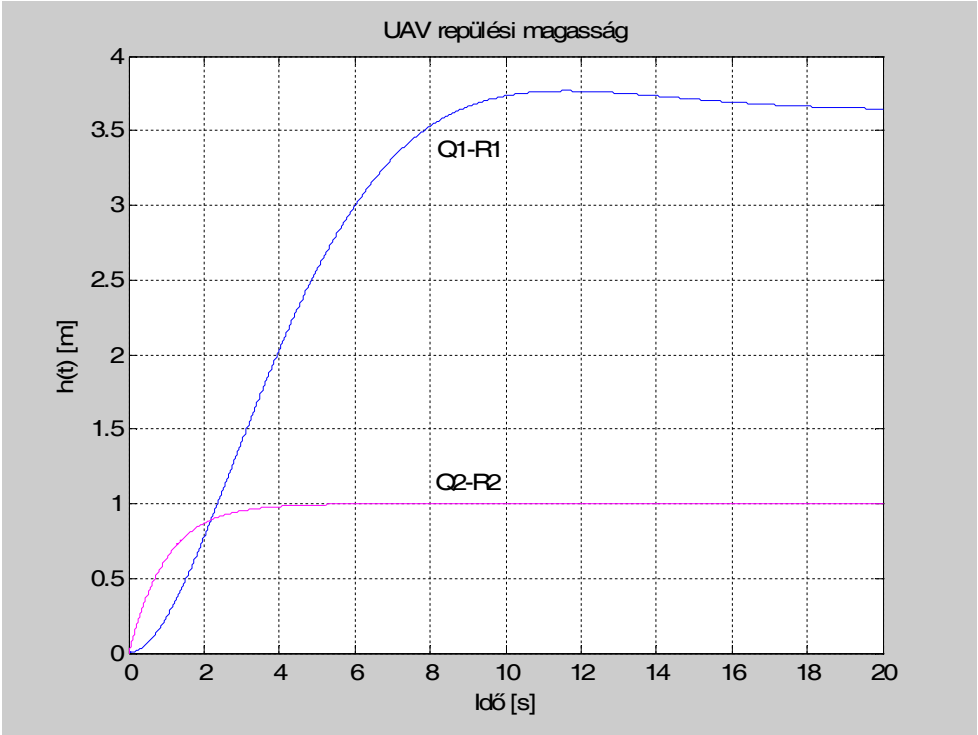


8. ábra. UAV zárt szabályozási rendszer átmeneti függvényei
Függőleges repülési sebesség Repülési magasság

Hasonlítsuk össze a két súlyozás alapján tervezett rendszer zárt szabályázási rendszer viselkedését. Az két rendszer megfelelő állapotváltozóit a különféle súlyozás alkalmazása esetére a 9. ábrán láthatjuk.



9. ábra. Az UAV zárt magasságstabilizáló rendszerének átmeneti függvényei.
UAV függőleges repülési sebesség (Q1-R1 Q2-R2)



9. ábra. Az UAV zárt magasságstabilizáló rendszerének átmeneti függvényei.
UAV repülési magasság (Q1-R1 Q2-R2)

A 9. ábrán jól látható, hogy az alapjel követés a $H_r(t) = 1(t)$ bemeneti jelre megvalósul, és a zárt szabályozási rendszer minőségi jellemzői is megfelelnek az előírt értékeknek [1, 2, 10, 11, 12].

5. ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A cikkben a szerző bemutatta a quadrotorok térbeli mozgásának matematikai modelljét, és az egyik, talán leginkább gyakori repülési üzemmóddal, a „függés” manőverrel foglalkozott. E manőverek során fő feladat a megadott repülési magasság tartása, a megfelelő minőségi jellemzők biztosítása mellett.

A repülési manőver optimális szabályozási rendszer segítségével is végrehajtható. Az LQR feladat megoldására a szerző új súlyozást mutatott be, aminek révén olyan szabályozó tervezhető, amely biztosítja a zárt repülésszabályozó rendszer előírt minőségi jellemzőit [12]. Az LQR feladat determinisztikus rendszerekre használható, így a cikkben bemutatott, és megoldott feladat kiterjeszthető sztochasztikus rendszerekre is, így a következő feladat a dinamikus szabályozó tervezése (az LQG feladat megoldása külső, és belső sztochasztikus zajok esetén) lesz. Ha szeretnénk robusztus szabályozási rendszert tervezni, akkor a robusztus repülésszabályozó rendszer tervezését a H_2-, vagy a H_∞ - módszerek segítségével végezzük el.

OPUS CITATUM

[1] MCLEAN, D., Automatic Flight Control Systems, Prentice-Hall International, New York-London-Toronto-Sydney-Tokyo-Singapore, 1990.

[2] NELSON, L. C., Flight Stability and Control, McGraw-Hill Companies, Inc., Boston, Massachusetts, Burr Ridge, 1998.

[3] SZABOLCSI, R., Egy felmérés margójára – néhány gondolat a pilóta nélküli repülőgépek polgári és katonai alkalmazásáról, Szolnoki Tudományos Közlemények XII., HU ISSN 2060-3002, 2008. http://www.szolnok.mtesz.hu/sztk/kulonszamok/2008/cikkek/szabolcsi-robert.pdf

[4] SZABOLCSI, R., Conceptual Design of Unmanned Aerial Vehicle Systems for Non-Military Applications, Proceedings of the 11th Mini Conference on Vehicle System Dynamics, Identification and Anomalies VSDIA 2008, ISBN 978-963-313-011-7, pp (637-644), Budapest University of Technology and Economics, 10-12 November 2008, Budapest, Hungary.

[5] SZABOLCSI, R., Some Thoughts on the Conceptual Design of the Unmanned Aerial Systems Used for Military Applications, XVI. Magyar Repüléstudományi Napok tudományos konferencia kiadványa, ISBN 978-963-420-857-0, BME, 2008. november 13-14, Budapest.

[6] SZABOLCSI, R., Conceptual Design of the Unmanned Aerial Vehicle Systems Used for Military Applications, Scientific Bulletin of "Henri Coanda" Air Force Academy, No. 1/2009., ISSN 2067-0850, pp(61-68), Brasov, Romania.

[7] SZABOLCSI, R., Identification of the UAV Mathematical Models, CD-ROM Proceedings of the VIth International Conference „New Challenges in the Field of Military Sciences, ISBN 978-963-87706-4-6, 18-19 November 2009, Budapest, Hungary.

[8] SZABOLCSI, R., Conceptual Design of the Unmanned Aerial Vehicle Systems for the Firefighter Applications, CD-ROM Proceedings of the 12th International Conference „AFASES 2010", ISBN 978–973–8415–76–8, p4, 27–29 May 2010, Brasov, Romania.

[9] SZABOLCSI, R., Conceptual Design of the Unmanned Aerial Vehicle Systems for the Police Applications, CD-ROM Proceedings of the 12th International Conference „AFASES 2010", ISBN 978–973–8415–76–8, p4, 27–29 May 2010, Brasov, Romania.

[10] Prof. Dr. Szabolcsi Róbert: Katonai robotok számítógéppel támogatott tervezése – QUADRO LAB szakmai műhely létesítése az új, nemzeti közszolgálati egyetemen, „Műszaki Tudomány az Észak-Kelet Magyarországi Régióban, 2011" tudományos konferencia kiadványa, 2011. május 18., ISBN 978-963-7064-25-8, pp(11-27), DAB Műszaki Szakbizottsága, Debrecen, 2011. — Plenáris előadás. http://store1.digitalcity.eu.com/store/clients/release/mtekmr_2011.pdf.

[11] Prof. Dr. Szabolcsi Róbert: Katonai robotok számítógéppel támogatott tervezése – QUADRO LAB szakmai műhely létesítése az új, nemzeti közszolgálati egyetemen, Multidiszciplináris Tudományok, HU ISSN 2062-9737, 1. kötet, 1. szám (2011), pp(31-42), Miskolci Egyetemi Kiadó, 2011.

[12] *MIL-STD 1797 A*, Notice 3, Flying Qualities of Piloted Aircraft, Department of Defense, Interface Standard, 2004.

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Németh Balázs
balazs.nemeth@upcmail.hu

A JÓ LOVAS KATONÁNAK... - A MONARCHIA EGYLÖVETŰ LOVASSÁGI PISZTOLYAI

Absztrakt

Dolgozatomban bemutatom a császári-királyi hadsereg lovassági pisztolyainak fejlődését a napóleoni háborúktól a königgrätzi csatavesztésig. A feldolgozott 60 év az elöltöltő-fegyverek korszakának utolsó hat évtizede, melyet gyors haditechnikai és harcászati fejlődés jellemez. Az 1830-as évektől számított három évtized alatt a sima csövű kovás elöltöltő fegyvert több lépcsőben felváltja a korszerű, egybeszerelt lőszert tüzelő, huzagolt hátultöltő lőfegyver. Dolgozatomban kiemelt figyelmet szentelek az 1848-49-es szabadságharc időszakának, a huszárok szerepének, tűzfegyveres harcászatának, kiképzésének.
Dolgozatom lényeges részét képezi a korabeli hadifegyverekkel végzett lőkísérlet, mely célja, hogy modern rövid lőfegyverek teljesítményéhez hasonlítva helyezzem el az elöltöltő lovassági pisztolyokat a kézilőfegyverek koordináta rendszerében.

The main objective of my work is to present the development of the cavalry pistols of the Habsburg Empire from the Napoleonic wars until the battle of Königgrätz. These six decades are the last phase of the development of the muzzle loading system. From 1830 the smooth bore flintlock military pistol is replaced by the modern metallic cartridge breach loading rifled firearms in several development steps. I also present the firearms tactics, training and role of the traditional Hungarian light cavalry, the Hussars during the rebellion of 1848/49.
The other objective of my work is to compare the last muzzle loading arms of the Habsburg Empire to modern firearms, by test firing them.

Kulcsszavak: *lovassági pisztoly, elöltöltő-fegyverek ~ cavalry pistol, muzzle loading system*

1. BEVEZETÉS

Ha van a világon olyan lovassági csapatnem, melyre elítélő pillantások nélkül rámondható, hogy magyar eredetű, akkor az a klasszikus könnyűlovas csapatnem, a huszárság. Hosszú történelmi hagyományokat ápolva alakult a magyar könnyűlovas harcmodor, mely oly sok ütközet sikeréhez járult hozzá a fegyvernem 19. századi második felében kezdődő hanyatlásáig. Fegyverei, harceljárásai nem sokat változtak a kuruc időktől a königgrätzi csatáig, s a „dali pár pisztoly" mindig is ott függött a nyeregkápa mellett, ahogy azt az ismert kuruc dal, a „Csínom Palkó, csínom Jankó..." is megénekli:

„Csínom Palkó,Csínom Jankó, csontos karabélyom
Szép csendes lódingom, dali pár pisztolyom
Nosza rajta jó katonák, igyunk egészséggel
Menjen táncba ki-ki köztünk az ő jegyesével„

A lovassági pisztolyok - és általában minden lovassági hideg- és tűzfegyver – a gyűjtők által legjobban túlértékelt militáriák. Keresett, vágyott darabok szinte egytől egyig, miközben harctéri szerepük erősen megkérdőjelezhető volt. Nyílt ütközetben, csatában nem vehette fel a versenyt sem a pisztoly, sem a karabély a gyalogság nagyobb hordtávolságú fegyvereivel. Imreh Sándor, volt Mátyás-huszár[1] erről így ír visszaemlékezésében:

1. ábra. Huszárok és ulánusok 1848-ból
Forrás: Ottenfeld

1Az 1848-49-ben megszervezett erdélyi 15. (Mátyás) huszárezred

„Marosvásárhelyen, Szászrégenen és Vécsen vonultunk keresztül Naszód felé. Naszódot elhagyva, emlékem szerint Szászbudakon, február 21-én délután pihenőt tartottunk egy pár óráig. Aztán folytatni akartuk utunkat tovább. Midőn a faluból kiindultunk, éppen alkonyatkor, s egy hegyen csendesen felfelé vonultunk, egyszerre csak dobpergést hallunk előttünk fenn a hegyen, az erdőszélen. Megálltunk azonnal és figyeltünk. Nem sokáig kelle várakoznunk, mert a másik percben egy hosszú csatárlánc (gyalogosokból álló) bukkant előnkbe a hegy mögül, s elkezdett reánk hevesen tüzelni. Naszód vidéki oláh határőrök voltak. Tüzeltünk mi is reájok karabélyaink- és pisztolyainkkal. E lőfegyverek azonban alig hordtak távolabb 100-150 lépésnél. Osztályparancsnokunk tehát visszavonulást vezényelt, mivel a lovasságnak gyalogsággal csatározást kezdeni nem tanácsos dolog." [1, 145 o.]

A lovasság fegyverzete mindig is változatos eszköztár volt. Különösen igaz volt ez a hagyományos magyar könnyűlovas, a huszár felszerelésére. A magyar huszár sokféle feladat ellátására volt alkalmas. Imreh Sándor így írja le a Württemberg-huszárok[2] felszerelését:

„Öltönyeik a következő darabokból álltak: fekete mente és dolmány, kivarrva gazdagon fekete-sárga vitézkötéssel, fekete csákó forgóval, kék posztóból készült feszes magyar nadrág a szükséges zsinórzattal, és magyar csizma nagy taréjú sarkantyúval. Legfelső öltönyük ujj nélküli nagy fehér gallérköpenyeg volt, mely zivataros, esős időben nem csak a huszárt magát, de a lovát is betakarta. Fegyverzetök: görbe kard, karabély és egy pár pisztolyból állt. A csinos tarsoly (a huszár zsebe), mely F.1. jeggyel volt jelölve (Ferdinandus primus); a kardszíjra volt erősítve, mely hátul a bal láb csizmaszárára leérvén, járás közben azt veregette. Tudni kellett ám azzal is járni, aki nem volt hozzászokva, mindegyre megbotlott benne. A gyakorlott huszár azonban tarsollyal is délcegen tudott járni." [1, 182 o.]

Legjobban a laza, harcrenden kívüli kötetlen harcmodor illeszkedett a magyar könnyűlovas virtusához, melynek része volt a meglepetés, üldözés, fogolyszerzés, cselvetés, felderítés, futárszolgálat volt, de adott esetben zárt kötelékben is tevékenykedhetett. [2]

A lovas katona kiképzésekor nem csak a kardvívásra helyeztek hangsúlyt, hanem a pisztoly biztos forgatására is: *„A katonai kiképzés mindig lóháton történt, egy-két napig nyújtófaszerű bottal tanulták a huszár hatvágást, majd két-három nap múlva már karddal tanulták a huszár hatvágást. Ehhez a hat vágáshoz, vagyis kardsuhintáshoz erős kar kellet, azért huszárnak többnyire erős embereket vettek be. Ezt abban állt, hogy villámgyorsan egy-két másodperc alatt úgy kellett a suhintásokat alkalmazni, hogy az ellenségnek először a két karját kellett levágni, majd a combra vágni és a kardot alulról felhúzva maguktól elfelé vágva, ezen utolsó vágással az ellenség fejét levágni... Mikor már tudták a hatvágást természetesen lovon ülve, és vágtatás közben kellett ezeket a vágásokat gyakorolni. Aztán megtanították őket, hogyan kell pisztolyt megtölteni, a puskaport, golyót vagyis lőni a pisztolyokból szintén lovon ülve tanulták. A puskaport, golyót, amely ólomból volt, zacskóban kapták és külön a gyutacsot, vagyis a kapsznit. A lövést ember nagyságú púpú vagy töltött zsák figurákra. Mikor egy-két hét alatt mindezt megtanulták, mentek a csoportokhoz, ahol az ütközetekbe csatákba vitték őket."* [3, 114 o.]- írja egy '48-as veterán visszaemlékezéseiben.

A lovassági harcászat legalapvetőbb egysége a század volt. Egy század két szárnyból, egy szárny két szakaszból (Zug-ból) állt. A századokat párban osztották be magasabb egységekhez. Ezek voltak az osztályok. Egy századhoz 150 huszár, a tisztek, és a kiszolgálók tartoztak.

A lóhátról történő viaskodásban a pisztoly sokkal inkább a védekezés fegyvere volt, mint a támadásé. A huszár ugyanis kivont karddal vágtatott rohamra, nem pisztollyal a kézben. A véres közelharcok nem tartottak sokáig, hogy a parancsnok ne veszítse el kontrollját egysége felett. Inkább kürtszóval megszakították a kézitusát, visszahívták katonáikat, újra sorakoztatták őket, és újra rohamoztak.

2A császári-királyi 6. (Würtemberg) huszárezred.

Nagyobb hasznát vette a könnyűlovas tűzfegyvereinek egyéb feladatainak ellátása közben. Nagyszerűen megfelelt a fegyver a portyázáshoz, lestámadásokhoz, cselvetésekhez. Karabélyát korlátozott távolságban, dragonyos szerepkörben, lóról szállva is használhatta.

A császári-királyi (k. k.) hadsereg és a honvédsereg lovasságánál azonos típusú fegyverek voltak rendszeresítve. Ezek vonalvezetése, pontossága nem sokat változott egészen 1859-ig, függetlenül attól, hogy milyen gyújtási móddal rendelkezett. Jelen írásunkban arra teszünk kísérletet, hogy bemutassuk a Duna-menti monarchia 19. századi elöltöltő lovassági pisztolyait.

2. LOVASSÁGI PISZTOLYOK A K. K. HADSEREGBEN

Az 1798 (1828), 1844 és 1859 M pisztolyok bár sok tényezőben eltérnek egymástól, mégis rengeteg azonos stílusjeggyel bírnak, melyeknek köszönhetően összetéveszthetetlenek más nemzetek hadi pisztolyaival. Az egyik ilyen fontos stílusjegy a markolat visszahajló, erősen íves formája, és az azt lezáró rézből - vagy a Lorenz pisztolyokon már acélból – készült markolatgomb. A lezáró alkatrész feladata nem egyszerűen csak az volt, hogy védje a fegyver sérülékeny részeit. Az erős fém alkatrésznek köszönhetően a pisztoly akár ütőfegyverként is alkalmazható volt végszükség esetén.

Szintén közös jegye e pisztolyoknak, hogy nem rendelkeztek töltővesszővel. A lovas katona vállszíjához rögzítve viselte a pisztoly és/vagy a karabély „putz-stock”-ot, ahogy azt a vadászok is tették. Így sokkal kisebb volt az esélye, hogy elveszítse lóháton történő töltés közben.

A három pisztoly alaptípus mindegyike egy-egy olyan névhez köthető, aki hosszabb-rövidebb ideig a bécsi arzenál parancsnoka volt: az 1798 M modellek Frh. Von Unterberger, a gyutacsos modellek báró Vincenz Augustin, a csappantyús modellek pedig Joseph Lorenz nevéhez köthetőek.

2.1. 1798 és 1798/28 M kovás lovassági pisztoly

2. ábra. 1798 M kovás lovassági pisztoly

Az 1798/28 M lovassági pisztoly adatai:

Teljes hossz:.	427 mm
Csőhossz:	263 mm
Űrméret:	17,6 mm
Tömeg:	1320 g

Az 1798-ban, a Frh. Von Unterberger javaslatára rendszeresített fegyverek között szerepelt az 1798 M típusjelű kovás lovassági pisztoly is. A vele egy időben rendszerbe vett lovassági karabélyhoz hasonló, de a gyalogsági puska lakatjánál kisebb kampós biztosítás nélküli kovás lakattal szerelték. Az ágyazat fája lenolajban áztatott diófa volt. A sárgaréz szerelékek és a

viszonylag keskeny ágyazat igen elegáns külsőt kölcsönöztek a pisztolynak. Valóban, az akkor ismert összes lovassági pisztolyok között az 1798 M a legtetszetősebb. Freiherr von Unterberger altábornagy, az 1796-os fegyverzeti bizottság elnöke így írt a lovassági pisztolyról:

„A pisztoly a kard után a lovas katona fontos és kényelmes fegyvere. Jobban kézre áll, mint a karabély, vagy a lándzsa, mert ehhez csak a jobb keze szükséges, míg a ballal a lovat tudja tartani. Egyébként nem terhes a viselésnél sem, mint a karabély, vagy a lándzsa." [4, 67 o.]

3. ábra. A főtöltet begyújtását a kova és acél által lángra lobbantott felporzólőpor biztosította

A pisztoly minden európai hadseregben hagyományosan a lovasság fegyvere, annak ellenére, hogy a találati pontossága, főleg lóhátról igen gyenge. A fegyver harci értéke eléggé korlátozott, mégis majd ötven éven át, kisebb változtatásokkal az osztrák lovasságtól elválaszthatatlan pisztoly maradt.

Az 1798 M kovás lovassági pisztoly lövedéke a csőnél jelentősen kisebb méretű gépi erővel gyártott, préselt – nem öntött - gömblövedék volt. A 8 vonás (17,56 mm) űrméretű sima csövekbe 7 vonás 3 pont (15,91 mm) átmérőjű gömblövedéket töltöttek, vagyis a lövedék és a csőfal között 1,65 mm hézag volt. A golyót a cső így precízen megvezetni nem tudta.

1828-ban a fegyver vonalvezetését, alkatrészeit egyszerűsítették. Változott a markolat formája, a lakatlemez profilja, a kakas formája, valamint néhány csavar pontos pozíciója is. Mindez az egyszerűbb gyártást szolgálta, de a módosítások a fegyver képességeit, hatékonyságát nem fejlesztették.

Az 1848-49. évi harcokban sok magyar egység harcolt még kovás fegyverekkel, lévén a szükség nagy úr volt, és a kovás fegyver sokkal jobb volt, mint tűzfegyver nélkül indulni a csatába, ütközetbe. Imreh Sándor, volt Mátyás huszár így ír erről visszaemlékezésében, az 1849. február 4-i vízaknai csatával kapcsolatosan:

„Feltűnt azonban nekünk nagyon, hogy honvédeink nem viszonozzák a tüzelést.

– Tüzeljetek bajtársak! – kiáltánk. – Máskülönben mind elesünk vagy foglyokká leszünk.

– Tüzelnénk bajtársak – válaszolának amazok –, de egyetlen töltényünk sincs.

– Miféle töltényekre van szükségetek? – kérdeztük.

– Kovás fegyverekhez valókra – válaszolának a honvédek.

Megjegyzendő, hogy Erdélyben a honvédség egy része gyutacsos-, a más része pedig kovás fegyverekkel volt ellátva. A mi, lovassági fegyvereink (karabélyok és pisztolyok) általán mind kovások voltak. A mi lőszereink pedig a gyalogsági fegyverekbe teljesen találtak. Ez nagy szerencse volt az alkalommal nagyon sokunkra nézve." [1, 103 o.]

Jó szolgálatot tett, hogy a lovassági tűzfegyverek és a gyalogsági tűzfegyverek mindegyike azonos méretű lövedéket tüzelt, így lehetővé téve a gyors gyártást, egyszerűbb logisztikát. A töltény lőportöltete 1 nehezék, azaz 4,37 g durva szemcséjű, lassú égésű muskétalőpor volt. A honvédsereg rendszerében a töltény csomagolásának színe fehér volt. Békeidőben a huszárok 10 töltényt és 4 kovakövet kaptak, míg hadi javadalmazásban 38 töltényt és szintén 4 kovát. [5]

2.2. 1844 M Augustin rendszerű, sima csövű gyutacsos lovassági pisztoly

4. ábra. 1844 M gyutacsos lovassági pisztoly

Az 1851 M lovassági pisztoly adatai:

Teljes hossza:	423 mm
Cső hossza:	251 mm
Kaliber.	16,9 mm
Súlya:	1550 g

Több szakirodalom úgy tartja, hogy az 1798 M lovassági pisztolyt csak későn, 1850-ben szerelték át az Augustin rendszerű kis gépi lakattal. Erich Gabriel monográfiája szerint tévesen beszélnek 1844 M típusú lovassági pisztolyról, mivel eddig még egyetlen pisztoly sem került elő, amelynek lakatlemeze 1852 előtti dátumot viselne. [4] Ezt az állítást cáfolja azonban, hogy mind Johann Joseph Wenzel Radetzky 1844. évi gyalogsági tábori utasítása, mind az 1848. évi honvéd gyalogsági tábori utasítások említik a perkussziós lovassági pisztolyokhoz rendszeresített töltényeket. [5]

A gyutacsos lovassági pisztolyok számos ponton megőrizték az 1798 M pisztolyok vonalvezetését: a réz markolatgomb, a jellegzetes réz csőtorkolat rögzítő, a sátorvas formája mint a korábbi modellt idézte. A lakaton kívül azonban számos apró különbségben el is tértek: a gyutacsos pisztoly ágyazása robusztusabb, a sátorvas talplemeze már acélból készült, mivel az 1798 M pisztolyok esetében gyakori volt a sátorvas hátsó nyúlványának törése. Egyik fegyver sem rendelkezett nézőkével, mindkét fegyver célgömbje a rézből készült torkolatrögzítő pánton helyezkedett el.

2.2.1. A gyutacs

5. ábra. A gyutacs elkészítése akár célszerszámok nélkül is lehetséges volt, így jobban megfelelt a honvédsereg igényeinek, mint a gépigényes lőkupak

A gyutacsgyártás egyszerűbb volt, mint a lőkupak gyártás. Az először káliumklorát és feketelőpor keverékével, majd később higanyfulmináttal töltött 15 mm hosszú, 3 mm átmérőjű rézhengert akár egy gyógyszerész is el tudta készíteni szükség esetén, s ilyen jellegű kreativitásra a honvédseregnek bizony sokszor volt szüksége.

A gyutacsok gyártása először a k.k. Feuerwerks Korps bécsújhelyi gyárában kezdődött meg. A gyártás folyamata a rézhenger elkészítésével kezdődött. A vékony rézlemez tisztítás után a vágógépek alá került, mely trapéz alakú formákat szúrt ki belőle. A kapott lemezt egy hengeres forma körül csővé hajlították, majd egyik végét a gép automatikusan lezárta összenyomással. A kapott hüvelybe egy következő speciális gép töltötte a csappantyúelegyet, majd megvizsgálták, hogy a kitöltés teljes-e. Ezt követően a hüvelyt lezárták, majd egy átmenő furatot alakítottak ki egyik végén a drót számára, mely a töltényhez rögzítette a rézhengert. A drótot szintén gép vágta megfelelő méretűre, és gépi erővel rögzítették a gyutacshoz is. Az így elkészített gyutacsokat felületükre felvitt lakkfestékkel konzerválták, hogy a levegő páratartalma ne károsíthassa az elegyet. Az így elkészített gyutacsok olyannyira vízhatlanok voltak, hogy még akkor sem veszítették el durranóképességüket, ha tartósan víz alá merítették őket. Ebből a szempontból korszerűbbnek mondható ez a gyújtási megoldás, mint a hagyományos egy oldalán nyitott kapszlik esetében. Ez utóbbinál a gyúelegy a rézcsésze fenekén helyezkedik el, kitéve a környezeti hatásoknak. [6]

2.2.2. Az 1844 M Augustin lovassági pisztoly tölténye

6. ábra. A császári-királyi hadsereg első kémiai gyújtású lakatja. Augustin-féle kis gép lakat

A magyar huszárság változatos feladatokat látott el mindig, így változatos fegyverzettel is rendelkezett. Tűzfegyver arzenáljának gerincét két pisztoly képezte, melyet a nyereg két oldalára szíjazott bőrtokban hordott. A sima csövű 1798 M kovás vagy a gyutacsos lakattal szerelt 1844 M Augustin pisztoly mindegyike elsősorban az önvédelem utolsó vonalát képezte. A lovas katona fő fegyvere kard volt, s ha olyan cudar helyzetbe került, hogy a hideg vas már nem tudta kimenteni, akkor nyúlt pisztolyaiért. De pisztolyt viseltek a tüzérségi szekerészet altisztjei, az aknászkar legénysége, a sajkások, a határőr ezredek tüzérei, a ménes és lópótlékozó osztály katonái, és az állatorvosi intézet legényei is.

A rövid fegyverek a gyalogsági puskák golyóját tüzelték hasonló konstrukciójú, de kisebb lőportöltetű papírtöltényekbe csomagolva, mint amilyeneket a hosszú fegyverek esetében megismerhettünk. A flastrom nélkül töltött 15,91 mm átmérőjű golyó alá 7/8 nehezék (59 szemer, 3,85 g) muskéta lőport töltöttek. A cső átmérője e fegyver esetében is 17,6 mm volt, így a pontos lövés e kombinációval sem volt biztosított, csak úgy, mint a kovás előd esetében.

7. ábra. A pisztoly ugyan azt a 24 g tömegű gömblövedéket tüzelte, mint a gyalogsági puska

A kémiai gyújtás intenzívebb, biztosabb, mint a kovás lakat gyújtása. A gyutacs szúrólángja a teljes lőportöltetet egyszerre képes meggyújtani, míg a kovás lakat belobbanó felporzólőporának lángja folyamatosan halad a lőportöltet aljától a lövedék feneke felé. A gyutacsos fegyver csövéből így azonos lőportöltet esetén is gyorsabban repül ki a golyó. A gyutacsos pisztolytöltény töltetét ezért csökkenteni lehetett 0,5 g-mal. Szintén indokolta a

csökkentést, hogy a töltet lőporából a katonának már nem kellett felporozni a serpenyőt, így a teljes töltetet a lövedék meghajtására tudta hasznosítani. A honvédsereg rendszerében a töltény csomagolásának színe fehér volt fekete kereszttel.

A pisztolyok önvédelmi fegyverek voltak, s hatásos viteltávjukat is mai léptékkel mérve igen kis távolságban jelölték meg:

„ Végtére a pisztolyokkal némi emelékkel valamelly pontossággal csak 25-30 (18-23 m – a szerz.) lépésnyire találhatunk.” [7]

A pisztolyok javadalmazása békeidőben 10 töltény volt, míg háborúban 32-38 töltény volt katonánként.

A tisztek – főleg ha tehetősebb családból származtak – nem a rendszeresített hadipisztolyokat viselték, hanem saját civil fegyvereikkel vonultak hadba. A szabadságharc számos legendás főtisztjének díszes fegyverei ma is megtekinthetőek múzeumainkban.

2.3. 1859 M (Lorenz) lovassági pisztoly (k. k. Kavelleriepistole M/1859)

8. ábra. 1859 M lőkupakos lovassági pisztoly

Az 1851 M lovassági pisztoly adatai:

Teljes hossza:	425 mm
Cső hossza:	260 mm
Kaliber.	13,9 mm
Súlya:	1400 g

A Duna-menti monarchia utolsó elöltöltő hadi pisztolya az 1859. évi típus volt, vagy közkedvelt nevén a Lorenz pisztoly. A robusztus egylövetű fegyver a kor normái szerint már szolgálatba állításakor is elavultnak számított, hiszen az 1850-es évek már bőven a hadi használatra is nagyszerűen alkalmas elöltöltő revolverekről szóltak. A Monarchia ennek lehetőségét bár vizsgálta, de a korszerű ismétlőfegyverek rendszeresítése helyett maradtak a régi, jól bevált robusztus nyeregpisztolyoknál.

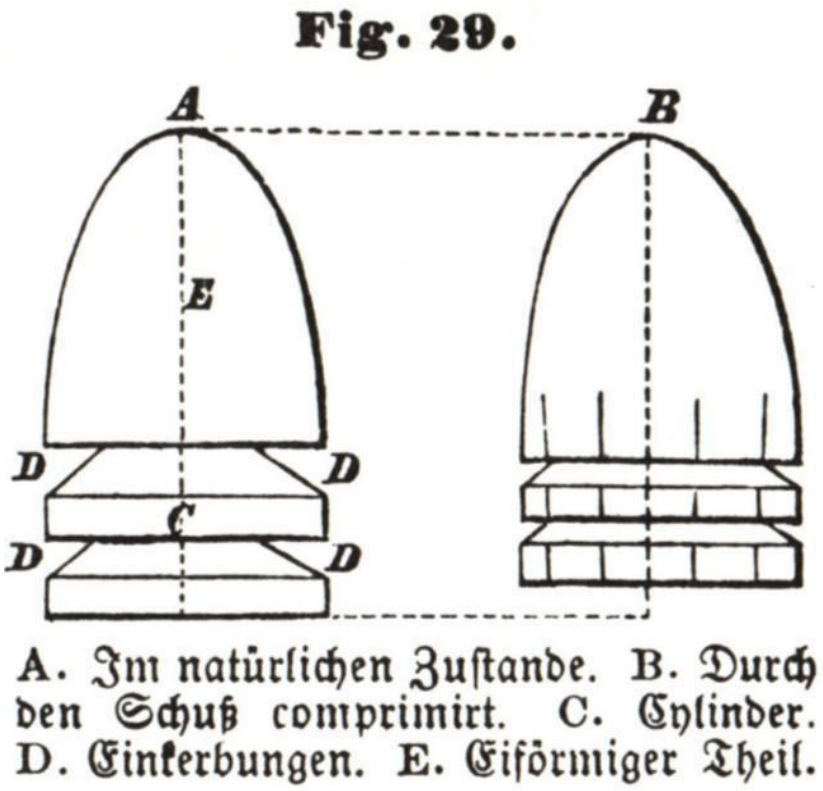
9. ábra. Gyutacsok_csappantyúk
Gyutacsok (balra) és lőkupakok (jobbra)

A fegyver lakatja már csappantyús, a négy szárnyú, 6 mm-es hadi lőkupakkal működött. A fegyver rendelkezik egy olyan ismertetőjeggyel, mely semelyik másik Lorenz fegyverre nem volt jellemző. A kakas nyugalmi állapotban biztosítható, így a lőkúpra visszaengedett kakas nem ért a csappantyúhoz. A fegyver így úgy volt szállítható, viselhető, hogy a lőkupak nem eshetett le a lőkúpról, de a fegyver még leesés esetén sem sülhetett el véletlenül. A biztosító a kakas hátrafeszítésekor automatikusan oldott.

10. ábra. A császári-királyi hadsereg csak későn, 1854-ben tért váltott a lőkupakos lakatrendszerre

A 13,9 mm, vagy régi osztrák mértékegység szerint 6''' kaliberű cső huzagolt, négy barázdával rendelkezik, mint a többi Lorenz lövedékek tüzelő hadifegyver. A spirál 83 cm-en fordult egyet, ez jóval gyorsabb, mint a fegyvercsalád bármely más tagja esetében. A gyorsabb spirálra elsősorban azért volt szükség, hogy a lövedék a rövid, 26 cm-es csőhosszon is kellő perdületet kaphasson. A csőfaron nem helyeztek el nézőkét, mindössze egy csőfaron és csőszakállon végigfutó hosszú V alakú bemarás segítette a lövészt. A célgömb fordított V profilú volt, így a két irányzék nagyszerűen illeszkedett egymáshoz. [8]

2.3.1. A Lorenz pisztoly tölténye



11. ábra. A Lorenz lövedék sokkal jobban tudta hasznosítani a lőpor energiáját mint a gömblövedék

A fegyver lövedéke az általános 13,7 mm átmérőjű kompressziós lövedék volt, ugyan az, melyet a gyalogsági puska, a vadászpuska, a lovassági karabély és a különcsapat puska tüzelt. A töltény azonban különbözött a 4 g lőportöltettel szerelt gyalogsági tölténytől. A pisztoly esetében a lövedéket 1,82 g lövészlőpor repítette ki a csőből. A lövedék és cső közti fojtást a faggyú és méhviasz olvadt elegyébe mártott papírtöltény palástja biztosította, így messze jobban illeszkedett a csőbe, mint a korábbi változatok lövedékei. A hosszú lövedék nem csak pontosabb volt, de nagyobb átütőerővel is bírt, mozgási energiáját jobban őrizte. [8]

A fegyvert két változatban készítették: biztosítóval és anélkül. Ahogy a többi osztrák-magyar fegyveren, úgy ezen is a lakaton elhelyezett három jegyű évszámbélyegző jelezte a gyártás évét.

A fegyver megőrizte az elődök masszív markolatformáját, de az ágyazás már a legtöbb esetben dióból készült, a szerelékek anyaga pedig réz helyett acél volt. A fegyver jellegzetes képéhez tartozik a markolatgombba rögzített gyűrű, mellyel a fegyvert a katona testéhez rögzíthette.

A Lorenz pisztoly két módosításon esett át rövid karrierje során, melyek közül a legfontosabb 1863-hoz köthető. Ettől az évtől kezdve a cső anyag vas helyett kovácsolt acél lett. A másik említendő változata az 1860 M pisztoly, mely annyiban tért el az 1859 M lovassági fegyvertől, hogy alkalmas volt tusa rögzítésére, így karabélyként is használható volt.

A fegyver ára jóval drágább volt a korábbi modelleknél, különböző változatai 17,75 és 19,25 osztrák gulden között mozgott. [9] Ez több, mint kétszerese az 1850 M gyutacsos pisztoly árának.

3. LORENZ VS. AUGUSTIN: 10 ÉV KÜLÖNBSÉG

A két fegyvertípust alig 10 év választja el egymástól a történelemben, mégis zongorázni lehet a műszaki jellegű különbségeken. Rekonstruálva az eredeti szolgálati haditölteményeket, összehasonlítottam a két fegyver szórásképét, pontosságát, valamint torkolati energiáját. A lőkísérlet bizonyos szempontból egyértelmű eredményt hozott, más szempontból azonban igen meglepő fejleményekkel szolgált.

3.1. Pontosság, energia

12. ábra. A Lorenz-féle pisztoly jóval pontosabb volt a huzagolt csőnek, és kúpos lövedéknek köszönhetően

Mindkét fegyverrel 21 m-re elhelyezett 4. sz. pisztolylőlapra lőttem feltámasztva, hogy azt a távolságot rekonstruáljam, mely a gyutacsos fegyverek lőutasítása szerint még ember méretű cél eltalálására alkalmas. A gyutacsos pisztoly a várakozásoknak megfelelően teljesített. Köszönhetően a csőnél 1,7 mm-rel kisebb tapaszolatlan gömblövedéknek, pontossága finoman szólva sem volt kielégítő. A lőlapot öt lövésből négyszer tudtam eltalálni. A fegyver visszarúgása igen komoly volt. A 24 g-os, 15,91 mm-es gömblövedéket 60 grain Swiss 2Fg lőporral töltöttem, amely korábbi, gyalogsági puskával végzett mérések szerint az eredeti töltetet megfelelően reprodukálni tudja. A lőpor jelentős mennyiségű égésterméket hagyott a csőben, így a harmadik lövésnél már ellenőriznem kellett, hogy rendesen lőporon van-e a golyó, annyira szorult. A lövedék sebessége 5 m-en 170 m/s körül mozgott, mozgási energiája ezen a távolságon 346 J volt, amely azért nem is olyan rossz, összemérhető egy mai 9x19 Parabellum pisztolylőszer teljesítményével. A lövedék igen gyorsan veszti energiáját, már 330 m távolságon leesik 100 J alá, amely érték a sebesítési képesség határa lehet ebben a kaliberben.

A Lorenz pisztoly természetesen jobban teljesített. 28 grammos kompressziós lövedékét 30 grain Swiss 3Fg lőporral töltöttem, amely térfogatra éppen a fele a gyutacsos pisztoly töltényének. A nehezebb kúpos lövedék azonban olyannyira jobban hasznosította a lőpor energiáját, hogy a kevesebb töltet ellenére is 210 m/s körüli sebességre volt képes 5 m-en. Az ehhez a távolsághoz tartozó mozgási energia 620 J körül volt, vagyis a modernebb lövedék fele annyi lőporral közel kétszer akkora energiára volt képes. Ez az érték kb. a modern .357 Magnum lőszerek alsó energia határának felel meg. A lőkupakos pisztoly pontosság tekintetében is lekörözte elődjét: az öt lövés szórása oldal irányban mindössze 13 cm-es szélességű volt, míg magasságban 30 cm. Ez utóbbi érték annak köszönhető, hogy nagyon nehéz a vékony nézőkét és a célgömböt megfelelő magasságban rendezni. A fegyver töltése

egyszerűbb volt, mint a gyutacsos pisztoly esetében: a koszolódás hatását nem lehetett érezni a leadott lövések során.

4. ÖSSZEFOGLALÁS

13. ábra. 70 év haditechnika történet egymás mellett

A három pisztoly összehasonlításakor a haditechnika fejlődésének fontos paradigmaváltásait érhetjük tetten. A 19. század egyre gyorsuló fejlődése szűk ötven év alatt felforgatta a harcászatot. A monarchia utolsó elöltöltő pisztolyai, a Lorenz pisztolyok már rég letűnt kort képviseltek szolgálatba állásuk napján is, annak ellenére, hogy egyesítették magukban a kor legfejlettebb technológiáit: huzagolt acél cső, lőkupakos lakat, ipari gyártástechnológiák. Kétségtelen előnye a korábbi változatokkal szemben. A fejlődés azonban nem volt teljesen organikus, a k.k. hadsereg egyszerűen kihagyta az elöltöltő revolverek fejlődési fokát, és 1870-ben a központi gyújtású egybeszerelt lőszert tüzelő a Gasser revolverek rendszeresítésével lépett szintet.

Felhasznált irodalom

[1] Imreh Sándor: Visszaemlékezés az 1848-49. évi szabadságharcra Erdélyben. Budapest, 2003.

[2] Csikány Tamás: Csata Komáromnál. Budapest, 2003.

[3] Dömötör Ákos: Hősök és vértanúk. Budapest, 1998.

[4] Erich Gabriel: Die Hand und Faustfeuerwaffen des Hapsburgischen Heere. Wien, 1994.

[5] Johann Joseph Wenzel Radetzky von Radetz: Feld-Instruktion für die Infanterie, Kavallerie und Artillerie. Wien, 1844.

[6] August Dub: Gewehre und munition den K. K. österreichischen linen-infanterie-regimentern. Wien, 1852.

[7] Tábori utasítás gyalogság, lovasság és tüzérség számára. Budapest, é.n.

[8] Hans-Dieter Götz: Militärgewehre und Pistolen der deutschen Staaten 1800-1870. Stuttgart, 1978.

[9] Anton Dolleczek: Monographie der k. u. k. österr.-ung. blanken und Handfeuer-Waffen. Wien, 1893-95.

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Horváth Zoltán

SYSTEM OF LOGISTICS TASKS IN THE CENTRE OF ECONOMIC SUPPLY IN THE DIRECTORATE OF THE NATIONWIDE CIVIL EMERGENCY PROTECTION OF THE MINISTRY OF INTERIOR AFFAIRS

Absztrakt/Abstract

A 2012. január 1-el létrejött egységes, integrált hivatásos katasztrófavédelmi rendszer létrejöttével szükséges újragondolni a katasztrófa-elhárítási logisztikai támogatás új rendszerét, és azon belül a BM Országos Katasztrófavédelmi Főigazgatóság Gazdasági Ellátó Központjának[1] (BM OKF GEK) helyét, szerepét a feladatok ellátásában. Cikkemben ezt az új feladatrendszert kívánom bemutatni, különös tekintettel a jövőbeli fejlesztések irányaira.

By establishing an official and fully integrated civil emergency protection system on 1 January 2012 it has become necessary to think over the new system of logistics, concerning prevention of emergency, as well as the role of the Centre of Economic Supply in the Nationwide Civil Emergency Protection of the Ministry of Interior Affairs[2] (furthermore BM OKF GEK) in fulfilling tasks. In my essay I would like to present this new system with special regards to trends concerning future development.

Kulcsszavak/Keywords: *katasztrófavédelem, logisztika, BM OKF GEK ~ emergency protection system, logistics, BM OKF GEK*

1 BM OKF Gazdasági Ellátó Központ önállóan működő és gazdálkodó költségvetési szerv, amely általános költségvetési gazdálkodási, pénzügyi és számviteli, továbbá vagyonkezelési feladatokat, valamint katasztrófavédelmi logisztikai támogató feladatokat (ellátás, gépjármű-üzemeltetés és szállítás, valamint raktár és készletgazdálkodás) lát el országosan és az ellátási területei irányába.

2 the Centre of Economic Supply in the Nationwide Civil Emergency Protection of the Ministry of Interior Affairs2 (BM OKF GEK) is an independently operating and managing budget organisation which provides tasks of general budgeting, finance, accountancy and management of property, as well as logistics tasks (supply, car-fleet operation and transportation, storage and stockpiling) nationwide and in the areas in their concern.

1. INTERPRETATION OF THE COMPLEX LOGISTICS SYSTEM OF CIVIL EMERGENCY PREVENTION

I consider defining the concept and aims of civil emergency protection as one of the results of my PhD research work.

The *concept* of logistics tasks in civil emergency protection:

„The logistics tasks in civil emergency protection consist of planning, organising, co-ordinating and managing activities which are accomplished in accordance with effective, necessary and suitable conditions of logistics tasks, as well as providing financial, technical and special sources in order to be applied in the most optimal way." [3]

The *aim* of logistics tasks in civil emergency protection:

„The aim of logistics tasks in civil emergency protection is to plan the necessary sources, to provide the necessary human, financial and technical conditions, as well as to organise and co-ordinate the application of these conditions in the process of prevention, protection and restoration." [4]

To accomplish the logistics tasks supporting the effective civil emergency prevention and protection, the system of logistics tasks must meet the following requirements:

- It must have a suitable integrating ability.
- It must be reliable and operative in all situations.
- It must provide the necessary speed and flexibility.
- It must have the suitable co-operative ability.
- It must be maintainable, financeable and cost-effective.
- It must make it possible to plan the processes of logistics tasks ahead, to provide the reliability of accomplishment. [1]

The sub-conditions of sources, needed for civil emergency protection are created and used during peacetime in the first place. The sources for wartime emergency protections tasks must also be planned during peacetime, which will obviously be used during preparations for a war and wartime periods.

It is also important to emphasize that sources needed for wartime activities *are connected to the elements of defense economy* within the system of interior military defense, planning and accomplishing such activities are basically involved in the interior military defense. Naturally, the elements of the sub-systems in civil emergency protection cannot be grouped in this form and in this sense, because there are such sources, (means, materials, equipment, etc.) whose purchase and usage is needed in peacetime as well as in wartime. [2]

The logistics tasks of civil emergency protection consist of three periods, i.e. prevention, rescue and restoration. At the same time it means to accomplish logistics tasks in BM OKF in normal periods, i. e. to provide human resources and the supporting logistics tasks in accordance with the Special Regulations of the Basic Law.

Based on the new civil emergency protection law which came into operation on 1 January 2012 the provision of purchasing logistics tasks in peacetime gets a greater emphasis. The OKF has to provide the necessary financial and technical means for prevention and training. At the same time the OKF is obliged to provide reinforcing support to civil protection organisations in the periods of rescuing. The logistics tasks of civil emergency protection are included in Table 1.

[3] Source: Dr. Tóth Rudolf-Horváth Zoltán: The role of logistics support in the nationwide system of civil emergency protection Polgári Védelmi Szemle 2009. Issue 1; page 155

[4] Source: Dr. Tóth Rudolf-Horváth Zoltán: The role of logistics support in the nationwide system of civil emergency protection Polgári Védelmi Szemle 2009. Issue 1; page 155

The areas of logistics support	Logistics tasks connected to civil emergency protection
Supply	Organising the tasks of rescue forces and all the other organisations concerned in the process of rescuing, as well as providing the evacuated inhabitants with the necessary conditions, accomplishing all the tasks connected to rescuing human lives and property
Financial support	Providing chemically protective materials, clothing, equipment, food supplies, industrial products, fuel and lubricants for the rescue forces and all the other organisations concerned in the process of rescuing, as well as for the evacuated inhabitants, organising all the tasks of supplying connected to the emergency
Technical support and repairs	Providing all the necessary informative, technical and computing equipment for the rescue forces, keeping it in full operation all the time
Transportation	Providing all the necessary materials, technical means for transporting rescue forces and all the other organisations concerned in the process of rescuing, as well as the evacuated inhabitants, accomplishing the tasks connected to damage statement with the help of the necessary materials and technical equipment
Storage	Stocking and storing of the equipment, materials and other means needed for aversion of the imminent danger, preparing the reception and distribution of national or international donations and aid-supplies
Management	Planning the implementation of logistics support in case of emergency by making a preliminary budget and energy resources, purchasing suitable and cost-effective stocks, defining the principles and requirements of application, supportive and management activities, validating the financial responsibility
Health care insurance[5]	Creating the conditions of health care and insurance for the casulties, the inhabitants in danger, as well as the rescue forces and all the other organisations concerned in the process of rescuing
Handling donations and aid-supplies	Handling, registering and co-ordinating the reception and distribution of national or international donations and aid-supplies

1. table. The areas of logistics tasks connected to civil emergency protection [3]

2. THE PECULIARITIES OF THE NEW LOGISTICS SYSTEM OF BM OKF

As for *logistics tasks*, the effectiveness of the management system of BM OKF can be enhanced if it is accomplished by a unified, central co-ordinating organisation. Naturally, this is basically an ability co-ordination which does not replace the commander task of the logistics management. With the help of such co-ordination, concerning logistics support parallelisms can be avoided, reporting and data-providing - supporting the operative logistics management - can be made more transparent. Regarding BM OKF the co-ordinating tasks would be required on the base of BM OKF GEK, where there is a versatile development of logistics abilities:

- working out methods and principles of supporting abilities in enhancing civil protection is under process at the moment (accomplishing tasks connected to training and equipping Hunor Mentőszervezet/Rescue Organisation),
- creating a defense stocklist based on common principles, in addition to this, a storage structure is also under process in which the civil logistics providers have an important role,

[5] The health care in emergency is not closely connected to the basic tasks of OKF.

- BM OKF GEK apply for purchasing more modern new defense equipment: mobile defense dams, containers, which will replace the existing ones,
- this year the incurrent items stored in the county storehouses will be gradually eliminated,
- allocating the remaining county storehouses under a central management.

BM OKF GEK must be ready to accomplish the logistics tasks of civil emergency protection. The provision of financial and human conditions needed for civil emergency protection is preliminarily the task of the state administration, nevertheless for effective accomplishment of these tasks, it is necessary to involve the sources of the organisational system. Suitable planning of activities is the pre-condition of effective protection, in which the financial and technical conditions for handling emergency situations are fixed, as well as prevention and all its conditions. [4]

We would like to involve into the new ability ensuring model of BM OKF the quickly reacting ability of the Regional Technical Rescue Bases (RMMB). The integration of RMMB, working in 24/48-hour-shift would make it possible to increase the number of defense stocks-to-be-deployed in the army posts by allocating containers of identical sizes.

The new system of technical graduation would adjust to this, whose operating principles can be summarized as follows:

1. The prior interfering forces are the ones in the surrounding county directorates of civil emergency protection which could be helped by the unit loads and transporting capacity found in the surrounding county directorates of civil emergency protection and the RMMB when necessary. These are the primary abilities[6]. We can also call primary abilities those of the central storage system which get into operation as a result of the decision of an operative team which will reach the territory in „the second wave".
2. In case the emergency escalates BM OKF GEK will get into action, that is the reinforcing logistics support will be deployed, which means involving the civil logistics providers and the transportation from the central storehouses of BM OKF GEK. Based on experience, the deployment of secondary logistics abilities can be planned 1-2 days ahead.
3. Simoultaneously, the ordering of insured stocks and replacing the consumed stocks would begin within the frames of the purchasing system of BM OKF GEK.

Finally, the suggested establishment of the co-ordinational task of logistics ability must be mentioned. It is necessary to create it as soon as possible. The civil emergency protection is a system in which the participants – in accordance with the suitable regulations – provide the civil emergency tasks with the help of their own organisations, sources and logistics tasks. Therefore it is unavoidable to create an organisational element on the basis of OKF GEK which provides co-ordinational management tasks, needed in the logistics support of the civil emergency protection.

The ability of co-ordinational activity shows a kind of similarity with the one of the supplying chain management. The basic aim of the supplying chain management is to optimise the co-ordination of logistics tasks of the organisations by creating as big value as possible. To set a good example, it is necessary to create a common purchasing, storing and transporting system in order to achieve an effective and economical operation. Based on the above mentioned ideas we can define the supplying chain management as follows:

[6] By prior ability we mean the common ability of the unit stocks (as supplies) and the transporting and handling abilities.

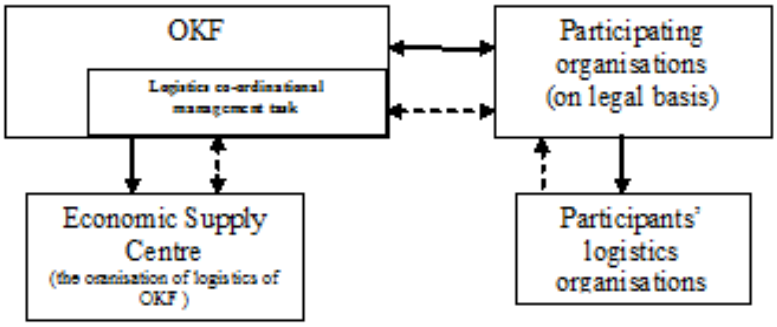
„The supplying chain management is the entirety of the co-ordinated managing and organising activities by material and information flow among the raw material suppliers, manufacturers and distributional providers and consumers who are closely connected to each other." [7]

Regarding BM OKF we can speak about the ability co-ordination of the logistics tasks among the civil emergency protection based on the civil emergency protection organisations and the Act of Law, concerning civil emergency protection. This co-ordination could be qualified for accomplishing the tasks of *primary and secondary logistics activities*[8].

Based on my research work done so far, by *primary logistics abilities* I mean the abilities of moving and using human resources, financial and technical sources, stocks, processes, methods (information flow) existing within the frames of the organisational sub-system, having its own abilities of logistics tasks. By *secondary logistics abilities* I mean the reinforcing and replacing logistics tasks, whose aim is to distribute the sources and means-to-be used in the area in danger directly, in due course, in the suitable quantity, with reinforcing ability, as well as to replace all the sources used by the organisations who take part in the rescue period. [5]

To sum it up, the aim of the whole co-ordinational activity is to meet the requirements of the above mentioned logistics supporting system by co-ordinating the primary and secondary abilities.

In this system it means as follows:



1. figure. The place of the logistics co-ordinational management task in the system of civil emergency protection [6]

This co-ordinational organisation would accomplish all the inner norma-creating tasks which are needed for the systematical operation of the civil emergency protection.

In operational periods:

- it would provide the co-ordination of the logistics supporting systems of all the participants, create and operate common logistics bases,
- it would provide the integrating task of civil and military logistics elements in the area of civil emergency protection,
- it would provide a permanent logistics ability monitoring which would be able to analyse the effectiveness of the protection from economic and financial points of view.

7 A concept made by the author is a summarizing statement which is based on the results of his research work, using the material of the lecture named Special Logistics by Dr. Tóth Rudolf, University Docent (ZNEBK416417-2008/2009. term I)

8 Interpretation of abilities see Horváth Zoltán: A new interpretation of national logistics support in civil emergency protection, Polgári Védelmi Szemle, Issue 2009/2, page: 120

3. CONSEQUENCES

My summary concerning the new logistics system of BM OKF GEK is as follows:

- logistics must be handled as a prior task by optimal allocating of the sources and abilities at disposal,
- the organising and resource-developing tasks must be accomplished already in the phase of prevention which will result in a well-prepared logistics supporting system,
- during the period of protection, an organisation, based on providing co-ordination could optimise the use of the logistics abilities, thus making it possible to use the necessary sources more effectively.

References:

[1] Dr. Tóth Rudolf-Horváth Zoltán: The place and role of logistics support in the national civil emergency protection, Polgári Védelmi Szemle, Issue 2009/1., ISSN 1788-2168, page 156

[2] Dr. Hornyacsek Júlia: Basic concepts of civil emergency protection 1., ZMNE University handout 2009. ISBN: 978-963-7060-66-3, page 130

[3] Table Horváth Zoltán: Logistics support of emergency aversion and elimination tasks, Műszaki Katonai Közlöny Year XX. (2010) ISSN 1219-4166, page 93 as well as

[4] Dr. Tóth Rudolf-Horváth Zoltán: The place and role of logistics support in the national civil emergency protection, Polgári Védelmi Szemle, Issue 2009. 1, ISSN 1788-2168; pages 156-157 Point *2.2* was written based on Chapter *The areas of logistics support in emergency aversions*.

[5] Dr. Hornyacsek Júlia: Basic concepts of civil emergency protection 1., ZMNE University handout 2009. ISBN: 978-963-7060-66-3, page 152

[6] Horváth Zoltán: A new interpretation of national logistics support in civil emergency protection, Polgári Védelmi Szemle, Issue 2009/2., ISSN 1788-2168, page 120

[7] Horváth Zoltán: A new interpretation of national logistics support in civil emergency protection, Polgári Védelmi Szemle, Issue 2009/2. szám, ISSN 1788-2168, page 123

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Petruska Ferenc
petruska.ferenc@unki-nke.hu

HÁROM ELFELEDETT HÁBORÚ

1. RÉSZ
SZOVJET-AFGÁN ÉS IRAK-IRÁNI HÁBORÚ

Absztrakt

A Magyar Honvédség szervezetében, felépítésében, feladatrendszerében az elmúlt évtizedekben jelentős változások mentek végbe, így kiváló eredményeket tudott felmutatni az afgán (MH Tartományi Újjáépítési Csoport) és iraki szerepvállalások során. Az új kihívások, új képességeket, modern technikákat, eljárásokat és speciális felkészülést igényelnek, amely irányainak megtalálásához a fenti két háborúban szerzett tapasztalatok is segítséget nyújthatnak.

Serious changes took place in the last two decades in the structure, tasks and organization of the Hungarian Army to achieve great success both in Afghanistan and Iraq. These brand new tasks require new types of capabilities, characteristic and modern techniques and training for which the consequences of these wars help finding the best solutions.

Kulcsszavak: *Irak, Afganisztán, hadászat, Szovjetunió ~ Iraq, Afghanistan, strategy, Soviet Union*

„A békefenntartás nem a katonák
feladata, azonban csak katonák
tudják elvégezni.”

(Dag Hjalmar Agne Carl Hammarskjöld, az ENSZ második főtitkára)

Soha sincs értelme háborús eseményeket előzményeik vagy következményeik nélkül vizsgálni, hiszen nem értenénk meg az ellenfelek céljait, elszántságát, túlkapásait, váratlannak tartanánk egyik vagy másik fél kiugrását vagy éppen belépését a háborúba, amit - valljuk be - a legjobb katonai szakértőknek is nehezen megy előre prognosztizálnia. Miért?

Mert a csatatereken egész egyszerűen közkatonák vannak "többségben", akiknek legtöbbször csupán sejtéseik vannak a háborúk okairól, a győzelem esélyéről és értelméről - gondoljunk csak a német-francia háborúkra, amelyeknek szinte egyenes következményeik a következő kirobbanása, amelyből az első a két országot, a második egész Európát, a harmadik szinte az egész világot lángba borította. És ez nem volt egyedül e két országra igaz, hiszen gondoljunk csak a cári Oroszország "háborúzási kényszerére", amelyet oly sokszor fogták fel a vezetők "presztízskérdésnek" vagy a keresztes háborúkra vagy akárcsak a katonai junta által vezetett Argentínára, ahol a feszültség levezetésének egy módját látták egy külső háborúban.

A motívumok vizsgálatakor legtöbbször anyagi érdekekre bukkanunk. Kezdetben egy jól termő terület, egy gazdag polisz[1] megfelelő indok volt a támadás megindítására. Persze a hadizsákmány soha sem oszlott meg egyenletesen ami - egy kis marxi túlzással meggyorsította a törzsi-nemzetségi keretek felbomlását - legalábbis feszültséget szült és máris kínálta a következő hadjárat indokát ....

Megmosolyogni való, de amerikai történészek szerint nagyon is komoly indoknak szolgált az Azték Birodalom számára az általuk oly sokra becsült madarak élőhelyeinek inváziója egész egyszerűen tollaik megszerzése érdekében! De ki tudja: lehetséges, hogy akárcsak egyetlen évszázad múlva ugyanilyen abszurdnak fog tűnni az a sok vallási-etnikai-anyagi-hegemonisztikai okokból véghezvitt vérfürdő, ami még napjainkban is elég százezrek, sőt milliók pusztulásához vagy "csupán" anyagi-erkölcsi-testi megnyomorodásához.

Talán a legfontosabb szempont napjainkban a harc kimenetelében, megelőzve a háborút irányító tényleges és propagált indokot és egy-egy nép lelki alkatát, a haditechnika. A két legfontosabb és mindenképpen forradalmi változás a következő: soha nem függött ennyire a harcok kimenetele a fegyverek fejlettségétől. Manapság elég egyetlen évtizednyi lemaradás a csúcstechnikától és a vereség elkerülhetetlen. A számítógépek és finommechanika oly gyorsan fejlődik, hogy az emberi tényező szinte teljesen fölösleges, sőt szinte az egyetlen, amely tévedhet. (Gondoljunk csak a NATO jugoszláviai beavatkozására, amelyet robotrepülőgépek[2] kezdtek meg.) A NATO legfelsőbb katonai vezetői közül viszont többen bevallották: egyedül levegőből kapitulációt elérni nem lehet. Tehát szükség van az "emberanyagra" a teljes győzelemhez, nem elég az egyértelmű légi fölény. De meddig?

A másik forradalmi változás viszont az adott hadakozó államok gazdaságával szemben állít fel minden eddiginél magasabb követelményeket: a mai csúcstechnika iszonyúan drága. Csak néhány példa: egy közepesen felszerelt harckocsi árából egy 1300 fős iskola építhető, egy modern bombázó 200-300 db második világháborús bombázóval ér fel. Nem csoda, hogy a Reagan elnök által a fegyverkezési versenybe hajszolt Szovjetunió "összeroskadt saját páncélja alatt..."

1 Hegyi Dolores, Kertész István, Németh György, Sarkady János Görög történelem – a kezdetektől Kr. e. 30-ig, Osiris, Budapest, 1995,ISBN 963-379-118-9

2 http://www.zmne.hu/kulso/mhtt/hadtudomany/2000/2_7.html (letöltve: 2012-02-05)

SZOVJET-AFGÁN HÁBORÚ

A régi Orosz Birodalomnak volt egy alaptétele, amelyet a Szovjetunió - úgy tűnik hagyományosan - megőrzött. Egy USA-beli Oroszország-szakértő[3] ezt a következőképpen fogalmazta meg: "A Kreml gyanakvó szeme csak csatlóst és ellenséget ismer és Oroszország szomszédjainak bele kell törődniük, hogy valamelyik szerepet kiosztják rájuk."

Ezen doktrína gyakorlati megvalósulására talán a legjobb példával Afganisztán szolgál.

Itt a Szovjetunóban kiképzett katonatisztek 1978. április 24-én megbuktatták a reformpárti miniszterelnököt, Daud herceget. Nur Muhhamed Taraki[4], aki az államcsíny idején börtönbüntetését töltötte, állam és pártvezető lett.

Az új afgán kormányt már a győzelem napján elismerte a Kreml. Tarakinek meglepően rövid idő alatt sikerült népköztársasággá alakítania az afgán államot.

Az „átalakítás" során viszont egyre nőtt a hagyományosan muzulmán lakosság ellenállása. A szovjet katonai szakértők segítségével sem lehetett az antikommunista erőket leverni. 1979 márciusában Herat városban a dühöngő tömeg elűzte a szovjetbarát vezetést, mire Moszkva harci helikoptereket bocsátott Taraki elnök rendelkezésére.

Kabulban ez év szeptember 14-én Hfizulláh Amin[5], Taraki alelnöke a forradalmi tanács gyűlésén meggyilkoltatta közvetlen felettesét és átvette a hatalmat. Amin azonnal hűségéről biztosította a Kremlt és felgyorsította a szociális átalakítást. Ez tovább fokozta az ellenállást. Több tartományban tört ki fegyveres felkelés, amelynek leverésében az afgán reguláris hadsereg tökéletesen haszontalannak bizonyult: katonák ezrei szöktek át a fellázadt ún. mudzsahedinekhez s persze magukkal vitték felszerelésüket .

A Szovjetunió rögtön észlelte, hogy Amin támogatásával kockára teszi egész Afganisztánt. Hogy ezt elkerülje, döntése intervenció volt.

Az afganisztáni bevonulás — még nyugati szakértők véleménye szerint is — úgy zajlott, akár egy hadgyakorlat: december 27-én elfoglalták Kabult és az ország összes lényeges stratégiai pontját, lemészárolták Amint és minisztereit, kaszárnyáiba zárták az afgán hadsereget. Külön említést érdemel a 105. légideszant-hadosztály, amely egyetlen éjszaka bevette a fővárost, majd olyan fontos pontokat, mint Herat és Sindand. Valószínűnek tűnt, hogy néhány héten belül egész Afganisztánt pacifikálják. Nem így történt...

Kiderült, hogy az odaküldött négy hadosztály nem elegendő a Babrak Karmal[6] által vezetett bábkormány megtartásához. Az ellenállás egyre erősödött, a reguláris hadseregből egyre többen álltak a felkelőkhöz. A mudzsahedinek egyre vakmerőbbek lettek: egyre többször támadták a szovjet hadsereget, hadtáposzlopokat, zsákmányoltak fegyvereket.

1980 januárjában újabb négy friss hadosztályt küldtek a térségbe: a 66., 201., 305. és 360. gépesített lövészhadosztályokat, amelyeket MiG-21 és MiG-23 korszerű harci repülőgépek biztosítottak. Érdekes, hogy mégsem ezek a pusztító erőben többszörösét képviselő repülők, hanem a Mi-24-HIND-D típusú harci helikopterek voltak a legjobb csapásmérők. Ezek alacsony repülésük során beszivárogtak a legeldugottabb gerillatáborokig, majd az ellenség bemérése után rakétákkal, nehézgéppuskával, esetleg napalmmal - a szó szoros értelmében - tűz alá vették az ellenséget. Az afgánok jobb híján gépfegyverekkel próbálták "leszedni" ezeket az egyébként páncélozott helikoptereket.

---

[3] George F. Kennan (1904-2005) amerikai tanácsadó, diplomata, politikus és történész

4 Nur Muhammad Taraki (1917. július 15 – 1979. szeptember 14.) afgán politikus és államférfi a Hidegháború idején.

5 Hfizulláh Amin afgán politikus és államférfi a Hidegháború idején, aki a széleskörű földreformokat hirdetett elnöksége idején.

6 Babrak Karmal (születési neve: Babrak Hashem; 1929. január 06 – 1996. december 03) afgán államférfi, aki arisztokrata származása ellenére kommunista elvek alapján kormányzott. mai napig nem tisztázott körülmények között halt meg Moszkvában.

A katonapolitikai cél a Kremlben borzasztóan egyszerűnek és könnyen kivitelezhetőnek tűnt: az egyértelmű technikai fölényre építve meg kell tartani a stratégiai pontokat, majd az afgán reguláris hadsereget felkészítése után azonnal harcba kell vetni, így elérhető, hogy a Szovjetunió a nemzetközi politikában "kívülállónak" hasson. Kudarcot vallottak…

Sem a megfélemlítés, sem a korszerűsítés nem sikerült, így kénytelen volt a szovjet vezetés saját kezébe venni a kezdeményezést. Csakhogy a szovjet hadsereg nukleáris, vegyi és hagyományos harci cselekményekre volt kiképezve!

Gerillaháborúra nem is számított a szovjet hadvezetés. Tankokkal próbáltak a kies afgán terepen győzelmet elérni. Az afgánok hamar megtalálták a megfelelő ellenszert, az aknát. Rendszeresen felrobbantották az előretörő harckocsi ékeket, majd a kellő zűrzavart kihasználva AK-47-es rohampuskákkal és RPG páncéltörőkkel tűz alá vették a szovjeteket.

Az áldozatok száma hirtelen megugrott, annak ellenére, hogy az USA megtorlásul csupán a moszkvai olimpiát[7] bojkottálta és az afgán irreguláris csapatok között szinte alig volt együttműködés. Az afgán reguláris haderő állapota viszont siralmas volt: légiereje csupán 167 db repülőgép, kevés páncélossal rendelkezett, csupán a kitűnő szovjet kézi fegyverek adták meg érdemi erejét.

A Szovjetunió harca "egyszerű" volt: "semleges" nemzetközi környezetben az afgán gerillák ellen.

Moszkva saját háborúját vívta kézzelfogható segítség nélkül kizárólag egyetlen, "láthatatlan" ellenfelével.

Hogyan voltak képesek az afgán gerillák ezt a hatalmas, kiválóan felszerelt és képzett hadsereget egyáltalán feltartóztatni? Mindenekelőtt ki kell térnem annak megemlítésére, hogy az ellátásuk fegyverrel és lőszerrel majdnem olyan tökéletes volt, mint az afgán hadseregé. Folyamatos ellátás érkezet Kínából, a rajtaütésekből, de kiváltképp Pakisztánból. Ellenállásuk három típusba sorolható[8]:

Első a déli területeken főleg a családfők által vezetett nemzetségi ellenállás. Egyébként itt volt a legmagasabb a veszteség.

A második az egy-egy falu területén állomásozó több száz főből álló jól felfegyverzett és kiképzett csapatok. Különös szokásuk volt, hogy lakóterületükön kívül ritkán bocsátkoztak harcba.

A harmadik típusú fegyveres alakulat a 20-50 főből álló, általában rajtaütésekkel és hadtáposzlopok elvágásával "foglalkozott".

Létszámuk állandóan változott 150 000 és 1 500 000 (!) között. Komoly előnyük volt - ebben hasonlítottak a Vietkong[9] harcosokra a legjobban - az a tény, hogy akár egy gyermek is potenciális harcossá válhatott tovább fokozva a szovjetek bizonytalanságát, hogy vajon ki is tekinthető ellenségnek és kik a "civilek".

A Vietkonghoz hasonlóan ők is mindenhol élvezték a "polgári lakosság" támogatását és kitűnő helyismerettel rendelkeztek. Óriási gyengéjük volt viszont a szervezetlenség, a korrupció - sok vezetőjük külföldre adta el fegyvereit -, kirívó képzetlenségük és az a tény, hogy minden nemzetség- vagy családfő csupán a maga kis territóriumának biztonságával törődött.

Moszkva lassan ráébredt, hogy hatalmas technikai fölényével sem tudja a háborút megnyerni. Egy tiszt így nyilatkozott a sajtónak: "sötét középkor ez és mi nem tudunk mit

---

7 Rózsaligeti László: Magyar olimpiai lexikon 1896–2002. Budapest: Helikon. 2004. ISBN 963 208 835 2

8http://www.biztonsagpolitika.hu/documents/1281893188_kovacs_lajos_orosz_afgan_haboru_-_biztonsagpolitika.hu.pdf

9 Dél-Vietnami Nemzeti Felszabadítási Front ellenálló szervezet volt, amely a vietnami háború idején az Egyesült Államok által támogatott Vietnami Köztársaság ellen harcolt.

Az amerikai katonák Vietkong („Viet Cong” (vietkong), illetve az amerikai katonák soraiban „Charlie”, „VC” vagy „Victor Charlie”) néven hivatkozott rájuk, amely a Việt Nam Cộng Sản, azaz „vietnami kommunista” kifejezésből ered.

kezdeni vele. A győzelem egyetlen módja lett volna, hogy helikoptereinkkel felperzseljük egész Afganisztánt benne összes lakójával. "[10]

Nem sokára sor került az 1988. májusi Taskentben tartott afgán-szovjet csúcstalálkozóra[11], amelyben megállapodtak a 40. szovjet hadsereg kivonásáról.

Ez a tény, akárcsak Vietnamban, előrevetette a rendszer összeomlását. Még sem ez történt: egyfajta patthelyzet jött létre az afgán reguláris és irreguláris erők között. Az események hátterében viszont 1 000 000 áldozat maradt, a helyzet viszont majdnem az volt, mint tíz évvel azelőtt....

A Szovjetunió nem szenvedett vereséget, de egyértelműen kudarcot vallott, meggyorsítva saját összeomlását. És ez a 14. fegyveres konfliktusa volt az első, amelyben szembesülnie kellett saját társadalma véleményével is...

AZ IRAK - IRÁNI HÁBORÚ

A 80-as években zajló fegyveres konfliktusok közül kiemelkedik veszteségeket és költségeket tekintve az iraki-iráni fegyveres konfliktus. Az évszázad egyik legjelentősebb háborús konfliktusává vált: csak a két világháború, a koreai háború előzi meg és egyenes következményévé vált az Öböl-háborúnak, hiszen az iraki hadsereget nem szerelték le a háború befejeztével. Hosszabb volt, mint a két világháború. Pusztítóbb, mint az összes arab-izraeli háború együttvéve!

Majdnem 2 000 000 katona harcolt az 1 200 km hosszú frontszakaszon[12].

A két érintett fél jelentősége főleg azon állt, hogy mindketten jelentős olajtermelő országok. Ez a tény nem csak az egész Öböl-térséget érintette volna rendkívül érzékenyen, hanem közvetve - az olajárrobbanás miatt - az egész Nyugatot, sőt, egyes történészek szerint akár a két szuperhatalom összecsapásához is vezethetett volna. Egy esetleges iráni győzelem megerősíthette volna az arab fundamentalistákat, ami több közel-keleti országban a mérsékelt iszlám kormányzat megdőléséhez vezetett volna.

De nézzük meg, mi történt ezalatt a harctereken.

Fontos elemezni, a harcok kimenetele szempontjából, milyen földrajzi adottságokkal és haderővel rendelkezik egy-egy ország. Ezek a tulajdonságok mutatják meg, hogy a villámháborús elképzelések - viszonylag kis területű, nagy haderejű és népsűrűségű támadó országnál - érvényesülnek-e vagy hosszú, stratégiai hadjáratot folytatnak. Ezek a 80-as években a következők voltak:

Maga a háború számos tekintetben sajátosnak mondható. Céljában és méretében korlátozott, de valamennyi hagyományos fegyver, sőt vegyi fegyver alkalmazásával folytatott, elhúzódó háborúról beszélhetünk, hosszabb hadműveleti szünetekkel[13].

Irak először lényegében védelmi jellegű hadászattal operált és nem használta ki harckocsikban, repülőgépekben és tüzérségben meglévő fölényét. A hadászati védelme arra összpontosult, hogy alacsony szinten tartsa harceszköz és élőerő-veszteségét, miközben jelentős veszteségeket okoz Iránnak. Ezáltal minimálisra csökkentette saját kiadásait és megpróbálta rávenni Iránt a háború kölcsönös befejezésére[14].

10

11 http://www.biztonsagpolitika.hu/documents/1281893188_kovacs_lajos_orosz_afgan_haboru_-_biztonsagpolitika.hu.pdf

12 Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 10. oldal

13 http://en.wikipedia.org/wiki/Iraq-Iran_War (letöltve: 2012-02-12)

14 Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 10. oldal

A hadászati védelem erősítése érdekében nagyszabású erődítési munkálatokat végzett az 1 200 km hosszú arcvonalon. Előszeretettel alkalmazták az elaknásítást, betonbunkereket, harckocsi és löveg tüzelőállásokat, a szögesdróttal való elkerítést.

Irán nagyobb népességére támaszkodva számolt azzal, hogy az iráni nép hajlandó lesz áldozatokat hozni a teljes győzelemért. Hadászati értelemben felőrlő taktikát alkalmazott, miközben tömeges élőerő rohamokkal jelentős veszteségeket okozott az iraki hadseregnek. Rendszerint nagy támadásokat indított az év elején, majd áttért rakéta és tüzérségi, valamint a tengeri rajtaütésekre.

A háborúban iraki részről vegyi fegyvert is alkalmaztak. 1984-ben iráni panaszt követően nemzetközi szakérők megállapították, hogy Irak mustárgázt és tabunt vetett be, amelynek kb. 10 000 sérültje lett. Időközben Irán is bejelentette, hogy képes vegyi fegyvert alkalmazni.

Iraki részről nagy előny volt, hogy megbízható utánpótlást[15] kapott minden fegyverfajtából. Kezdetben a legnagyobb szállító a volt Szovjetunió volt, majd amikor az szállítmányait felfüggesztette Franciaország, Kína, Korea és Egyiptom lépett a helyébe.

Iránnak nem voltak ilyen megbízható forrásai, de így is hozzájutott korszerű fegyverekhez. Sőt, hozzávetőlegesen 19 milliárd (!) dollárt[16] költött az adott időszakban fegyverekre. Importálói között ott volt az USA, a Szovjetunió és még Izrael is!

Irakot segítették egyiptomi önkéntesek[17] (17 000 fő!) is. De más államok fiai is együtt meneteltek iraki katonákkal, akik kiképzést is kaptak. Szaúd-Arábia például repülőtereit bocsátotta Irak rendelkezésére, hogy az onnan iráni célpontokat támadhasson.

A térségben található államokat arra kényszerített a háború, hogy saját hadseregüket korszerűsítsék. Növelték a fegyveres erőik létszámát, hogy a fegyveres konfliktus ki ne terjedhessen rájuk, vagy ha igen, eredményesen védekezhessenek.

1984-től Irak összehangolta[18] az állóvédelmet a légitámadásokkal és az olajszállítók elleni csapásokkal. Azt remélte, hogy ezzel megfosztja Iránt olajbevételeitől és az egyébként is ránehezedő nemzetközi nyomás hatására rászorítja a tárgyalásos rendezésre.

1986 előtt az iraki légierőt az jellemezte, hogy kisebb kötelékek bevetésével, nagy magasságokból dobtak le bombákat, ami nagyon korlátozott eredményre vezetett. 1986-tól megkezdte komoly romboló hadjáratát. Sokkal több felszállást hajtott végre, nagyobb távolságokra mért csapásokat, agresszívabb, pusztítóbb, egyszersmind kockázatosabb eljárást alkalmazott katonai, gazdasági és közlekedési célpontok ellen.

1988 tavasza fordulatot[19] hozott a háborúban. Az iraki hadsereg eredményesen használta ki az esős évszak lehetőségeit. Lendületes ellentámadások sorozatával minden, korábban Irán által elfoglalt területét visszafoglalta, sőt némi térnyerésével lehetővé tette a háború befejezését.

1988. július 18-án Khomeini Ajatollah[20], az iráni vezetők javaslatait meghallgatva, elfogadta az ENSZ Biztonsági Tanácsának - korábban hozott - az iraki-iráni háború befejezését célzó 598. számú tűzszüneti határozatát[21], amelyet Irak már egy éve elfogadott.

---

[15] http://en.wikipedia.org/wiki/Iraq-Iran_War (letöltve: 2012-02-12)

[16] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 11. oldal

[17] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 11. oldal

[18] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 11. oldal

[19] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 12. oldal

[20] Ruholláh Muszavi Homejni iráni síita vallási vezető (ajatollah, mardzsa), az 1979-es iráni forradalom egyik vezéralakja majd Pahlavi elűzésétől haláláig a „forradalom vezetőjeként" Irán államfője volt. Khomeini a dzsihád hirdetője - a szó mindkét: a szent háború és az iszlám hívő önmegtagadó, belső harca értelmében is. Az egész iszlám világban hatalmas tekintélyre tett szert.

[21] United Nations Security Council Resolution 582

A külföldi szakemberek levonták az alapvető következtetéseket[22]:

- Komoly előny volt a védelem kiépítettsége;
- Tartalékok, önkéntesek és helyi erők jelentősége kiemelkedő volt;
- Korántsem volt a technikának - F-14 harcrepülőgépeknek és az ultramodern MiG-25-nek - olyan jelentősége, mint az egyszerű kézifegyverekkel felszerelt, lelkes katonák tömegeinek.
- A bonyolult fegyvereket ritkán alkalmazták tömegesen, hiszen hiányos volt a kezelők képzettsége és a technikai utánpótlás is.
- Gyenge volt a vezetés, a képzettség és az ellenőrzés, valamint a hadászati - harcászati szervezés és tervezés.

De az iraki-iráni háborúnak alig lett vége és máris egy újabb konfliktus körvonalai rajzolódtak ki...

IRODALOMJEGYZÉK

[1] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest)

[2] Magyar Hadtudományi Társaság: Hadtudományi Lexikon (Akadémiai Kiadó, 1995)

[3] Weiszhár Attila – Weiszhár Balázs: Háborúk lexikonja (Atheneaum Kiadó, Budapest 2004.)

[4] Dr. Horváth Csaba: Az 1945 utáni legjelentősebb helyi háborúk és azok tapasztalatai (Zrínyi Miklós Nemzetvédelmi Egyetem nyomdája, 1999)

[5] Nagy Károly: Nemzetközi jog (Püski, Budapest, 1999)

[6] Ádány-Almási-Baller-Balla-Géczy-Harai-Hegedűs-Horváth-Kussbach-Rátkai-Törő-Varga: A fegyveres összeütközések joga (Zrínyi Kiadó, 2009)

[22] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 12. oldal

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Petruska Ferenc
petruska.ferenc@unki-nke.hu

HÁROM ELFELEDETT HÁBORÚ

2. RÉSZ
AZ ÖBÖL-HÁBORÚ

Absztrakt

A Magyar Honvédség szervezetében, felépítésében, feladatrendszerében az elmúlt évtizedekben jelentős változások mentek végbe, így kiváló eredményeket tudott felmutatni az iraki szerepvállalás során. Az új kihívások, új képességeket, modern technikákat, eljárásokat és speciális felkészülést igényelnek, amely irányainak megtalálásához a fenti háborúban szerzett tapasztalatok is segítséget nyújthatnak.

Serious changes took place in the last two decades in the structure, tasks and organization of the Hungarian Army to achieve great success in Iraq. These brand new tasks require new types of capabilities, characteristic and modern techniques and training for which the consequences of this war help finding the best solutions.

Kulcsszavak: *Irak, hadászat, Egyesült Államok, Öbölháború ~ Iraq, strategy, USA, Gulf-war*

AZ ÖBÖLHÁBORÚ

Irak az Iránnal vívott háború folyamán egy közel kétmilliós hadsereget szervezett meg, amit a tűzszünet ellenére nem fegyverezett le. Egy ilyen méretű katonaállomány fegyverben tartását a remélt béke nem tette volna indokolttá. Az iraki határon tevékenykedtek ENSZ megfigyelők is, közöttük 15 magyar honvédtiszt[1], akik megbízhatóan ellenőrizték a tűzszünet betartását. Irak biztonságérzetét az is indokolni látszott, hogy csapatait az országon belül mélyen hátravonta.

Az a nyilvánvaló tény viszont, hogy Irak nem szerelte le hadseregét előrevetítette egy újabb háború kitörésének árnyékát. Ennek konkrét célját nehéz volt meghatározni, hiszen a háború befejeztével az iraki vezetés is reménykedett abban, hogy sikerül megszereznie a szuverenitást Shatt-al Arab régió felett.

Az események 1988 augusztusában Kuvaiti kezdeményezésre tárgyalások kezdődtek a két ország közötti végleges határ kijelöléséről.

1989. július 26-án Irak nyíltan megfenyegette Kuvaitot, amelynek egy 400 000[2] fős csapatösszevonással adott nyomatékot. Az összevonást nyíltan hajtotta végre, mégis mindenki csupán beugratásként tartotta számon, amellyel presszíót akar gyakorolni Kuvaitra. A későbbi eseményekből viszont már nyilvánvalóan következtethetünk arra, hogy a támadás terve már elkészült és Kuvait lerohanását már Irak elnöke eldöntötte.

Irak tudta, hogy lépését nemzetközi tiltakozás fogja követni és az USA katonai ellenlépése sem kizárt. Erre utal az a később nyilvánosságra került tanulmány, amelyben széleskörűen tanulmányozták egy esetleges Irak-USA háború valószínű kimenetelét, de ara a következtetésre jutottak, hogy a nyilvánvaló technikai lemaradás ellenére legalább a szárazföldi közelharcban feltartóztatják majd az amerikaiakat[3]. Arra viszont egyáltalán nem számított Irak, hogy a nemzetközi közvélemény - közte több arab országgal - ilyen egységesen elítéli majd az inváziót, sőt határozott és súlyos szankciókat hoznak majd vele szemben.

Irak számított arra a lehetőségre is, hogy az ellene folyó háborút majd egy arab-USA vagy egy ötödik arab-izraeli háborúvá szélesíti majd és apellálva a nyugati pacifista közhangulatra - akárcsak Vietnámban - békére szoríthatja az USA kormányát.

A válság egyre inkább a fegyveres konfliktust valószínűsítette, különösen azután, hogy Irak sorozatosan visszautasította az ENSZ Biztonsági Tanácsának követeléseit. A háború kirobbanását valószínűsítették a következő tényezők[4] is:

1. Egy viszonylag kis területen óriási hadpotenciál halmozódott fel.
2. Irak nem jutott semmilyen előnyhöz az iráni agresszió folytán.
3. Az iraki elnök nehezen viselte el a kudarcot. Ezt példázza az iraki-iráni háborúban mutatott "példás" kitartása is.

A közel-keleti térségben már egyébként is jelenlévő konfliktusok a fegyveres megoldást inspirálták.

De mi is volt ennek a háborúnak közvetlen célja? Ezen kérdés megválaszolásához fontos az ENSZ Biztonsági Tanácsának követeléseit[5] vizsgálni.

---

[1] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 13. oldal
[2] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 13. oldal
[3] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 13. oldal
4 Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 13. oldal
5 A legelső a 660. számú határozat volt, amely elítélte Irak agresszióját és követelte a kivonulást, valamint a tárgyalások megkezdését. A legutolsó, 678. számú határozatot november 29-én hirdették ki, amely jóváhagyta „minden szükséges eszköz” alkalmazását az iraki hadsereg kiűzésére, amennyiben azok a megszabott határidőig önként nem távoznak. A határidő 1991. január 15. 24:00.

Az USA a Reagan[6]-időszaktól megkezdett hadikorszerűsítés és vezetés-irányítás legkiforrottabb és legkorszerűbb módszereit vetette be Öbölháborúban. A parancsnokok és közkatonák a háborút megelőző fél évben összekovácsolódtak és tapasztalatokat szereztek. A harcoló csapatok sivatagi körülmények között, Szaúd-Arábiában és Nevadában készültek a harcra a leendő harccselekmények körzetét és a stratégiai objektumokat imitáló, csaknem a valóságnak megfelelő hűséggel imitáló lőtereken. A lehetséges légi csapások valamennyi változatát a hajózó állomány a terepen, valamint reális körülmények között gyakorolta be.

1990 novemberére aktívvá vált az Amerikai Központi Parancsnokság 7.

Decemberre létrehozták a szövetségesek fő hadászati-hadműveleti csoportosításait: a keleti támadó csoportosítást, az északi támadó csoportosítást és az észak-nyugati különleges harccsoportot, amelyekbe amerikai, brit, francia, valamint az arab szövetségesek kijelölt erői tartoztak. Szövetséges erők légiereje, amelynek alapvető részét az USA légierő képezte, a legerősebb és legkorszerűbb harcászattal rendelkező erő volt. Csoportosítása három irányból, észak-nyugatról, nyugatról és délről tette lehetővé a légicsapások végrehajtását az Irak központi és déli körzeteiben elhelyezkedő objektumok ellen, valamint Kuvait térségében.

A szövetséges haditengerészeti csoportosítás gerincét, csaknem 140 hadihajót s benne 7 repülőgép-hordozót, anyahajót és 8 tengeralattjárót számláló amerikai, francia és angol erőt, valamint az amerikai tengerészgyalogság alkotta. Ezt kiegészítette a 18 résztvevő országból kijelölt mintegy hetven fregatt, romboló, aknaszedő, korvett, partvédő, kísérő és kisegítő. A teljes támadó csoportosítást a szövetségesek 1990 végéig hozták létre. Az iraki katonai vezetés megtévesztésére azonban a teljes készenlét elérését az amerikai hadvezetés hivatalos nyilatkozataiban február végére jelezte. Az iraki felderítés gyengeségei és rossz helyzetértékelés miatt viszonylagos váratlanság biztosítva volt.

A háborúra való katonai felkészüléssel párhuzamosan intenzív politikai és diplomácia tevékenység folyt, annak érdekében, hogy békés módszerekkel kényszerítsék Irakot az ENSZ BT november 29-én hozott 660-664. számú határozatainak végrehajtására. Ezeknek lényege az iraki hadsereg végleges távozása Kuvait földjéről 1991. január 15-ig. Mivel a Biztonsági Tanács által meghatározott határidő lejárt és Irak nem vonult ki Kuvaitból, 1991. január 16-án hivatalosan kinevezték a Szövetséges Erők Főparancsnokának Richard Cheney[8]-t, valamint a Hadműveleti Területek Főparancsnokának Normann Schwarzkopf tábornokot. A többnemzetiségű csapatok vezérkarai között együttműködést Colin Powell[9]

---

6 Ronald Wilson Reagan (1911. február 6. – 2004. június 5.) színész és politikus, Kalifornia állam kormányzója, az Amerikai Egyesült Államok 40. elnöke. Hazájában úgy tartják, kulcsszerepe volt a Szovjetunió megdöntésében, amit a „Gonosz Birodalmá”-nak nevezett. Népszerűségére jellemző, hogy az 1984-es választáson Reagan minden egyes államot megnyert, Minnesota kivételével. 1989-ben, mikor befejeződött második elnöki mandátuma, saját alelnökét, Busht ajánlotta utódjául, ezzel is biztosítva politikájának folytatását.

7 US Central Command, USCENTCOM

8 Richard Bruce „Dick” Cheney (Lincoln, Nebraska, 1941. január 30. –) az Amerikai Egyesült Államok 46. alelnöke George W. Bush elnöksége alatt. A Fehér Ház alelnöki hivatalának vezetője („Chief of Staff”), az amerikai képviselőház tagja Wyomingból és az USA védelmi minisztere volt.

9 Colin L. Powell (1937 április 5-én született New Yorkban) 35 évig volt hivatásos katona.

1989 októberétől 1993 szeptemberéig a vezérkari főnökök egyesített tanácsának elnöke - az amerikai hadsereg legmagasabb szintű vezetőjeként 28 katonai konfliktust vezényelt, így például az 1991-es Öböl-háborút.

A Bush kormány mérsékelt tagjai közé tartozott. Amikor 2002-ben az első riasztó jelentések beérkeztek az Iraki arzenál különböző fejlesztéseiről Dick Cheney alelnök és Donald Rumsfeld hadügyminiszter gyors katonai közbelépést sürgettek - Powell viszont azt javasolta, hogy vegyék fel a kapcsolatot az ENSZ-szel. Powell elképzelése, miszerint Iraknak adni kell egy utolsó esélyt a leszerelésre, a fegyverzetellenőrök révén valósult meg.

Saját katonapolitikai doktrínát alakított ki az amerikai hadsereg külföldi bevetésével kapcsolatosan. A doktrína szerint a katonák csak akkor vethetőek be, ha egyértelmű nemzeti érdeket kell védelmezniük és tudják, milyen feltételek esetén lépnek ki a háborúból. Továbbá: az amerikai csapatokat túlerőben kell bevetni, csak akkor, ha a siker biztos.

tábornok koordinálta. Bush[10] elnök 1991. január 16-án személyesen adta át az elnöki direktíváját a főparancsnokoknak a "Sivatagi Vihar" hadművelet megindítására. Ezzel megkezdődött a Második Világháború utáni legnagyobb méretű háború. A "Sivatagi Vihar" hadművelet 1991. január 16-án 22:40-kor erős elektronika "csapásméréssel", a szövetségesek rakéta-, sorozatvető és nagy hatótávolságú ütegeinek félórás - az iraki határtérségben elhelyezkedő légvédelmi elemeire mért - pusztító erejű tűzcsapásaival, a tengeri telepítésű és repülőgép-fedélzeti manőverező robotrepülőgépek, valamint a "Lopakodó" F-117A bombázók nagy pontosságú fedélzeti fegyvereivel végrehajtott légicsapásaival kezdődött meg. A Második Világháború óta példátlan bombázás már ekkor eldöntötte a háború kimenetelét…A háború első 34[11] napján önálló légi hadműveletek folytak. A szárazföldi csapatok tevékenységére csak kisebb erőkkel, regionálisan és komoly légi támogatással került sor. A szövetséges légierő fő feladata volt a hadászati légi fölény kivívása.

A légi hadjárat három időszakra bontható.

Az első időszak 1991. január 16. és január 21. között zajlott, amikor a szövetségesek a légi fölényt kivívták és kedvező feltételeket hoztak létre az iraki katonai vezetés és légvédelmi rendszer tevékenységének megakadályozására. Ezután lehetővé vált Irak hadpotenciáljának pusztítása, hadászati tartalékok (pl. Köztársasági Gárda[12]) erőinek a pusztítása.

A második időszak 1990. január 22-től február 23-ig tartott. A légi fölényt a szövetségesek sikeresen megtartották, Irak hadiiparát tovább gyengítették és Kuvaitban és Dél-Irakban kibontakozott hadműveleti csoportosítását bombázták. A fölényt február végére biztosították, az iraki hadsereg utánpótlási lehetőségei a minimumra csökkentek, így a légierőt a szárazföldi csapatok pusztítására, valamint a szövetséges haditengerészeti erő partraszállása érdekében és a szövetséges csapatok előrevonásának biztosítására használták. A légtámadások ereje és intenzitása óhatatlanul civil áldozatokat[13] követelt.

A szövetségesek haditengerészete Kuvait partjánál rakéta- és tüzérségi tűzcsapásokkal, légierejének légicsapásaival pusztította a partvédelmet és egyéb iraki célpontokat.

A légi hadműveleteket a felszabadító erők február 22-től ismét felújították és ekkor a szövetséges légierő - a szárazföldi csapatok ütközetbe vetését előkészítve - tömeges légitámadásokat hajtott végre a harcászati tartalékot képező, Kuvait észak-nyugati részén levő páncéloshadosztály, valamint a tartalékot képező, Irak déli részét védő Köztársasági Gárda, a Bagdad és Baszra körzetében levő objektumok és Irak partvédő erői, valamint nagyvárosai ellen. Eközben Irak február 1-jén éjszaka — a szövetségesek számára váratlanul — bevetett több mint ezer harckocsit és közel ötszáz páncélozott járművet, valamint 60 000 főt számláló szárazföldi csoportosítását Kuvait területéről Hafdzsi város irányába.

---

[10]George Herbert Walker Bush (Massachusetts, Milton, 1924. június 12.) az Amerikai Egyesült Államok 41. elnöke (1989–1993). Korábban ENSZ-nagykövet, CIA-igazgató, illetve – Ronald Reagan elnöksége alatt – alelnök (1981–1989). Miután Irak megszállta Kuvaitot, az amerikaiak számára veszélyessé vált a korábbi szövetséges állama. Bushnak sikerült meggyőznie a közvéleményt és az ENSZ-et a háború szükségességéről. Jóllehet, a háború után Bush népszerűsége magas volt, hivatali idejének végére nyilvánvalóvá vált, hogy az ország belső, gazdasági problémáira nem tudott megoldást találni. 1992-ben, döntően emiatt, nem sikerült újraválasztatnia magát.

11 Dr. Csabai György CSs: Visszatekintés az 1990-1991-es Öböl-háború tapasztalataira (letöltve: 2012-02-05)

12 A Gárda legfontosabb feladata békeidőben az volt, hogy megóvja a vezetést a katonai puccsoktól. Az iraki átlaghoz képest jól felszerelt egységei voltak, hogy a pontosan megtervezett, elsősorban logisztikai kihívást jelentő ütközeteket vívják meg. A Gárda harci ereje, bár iraki viszonylatban kimagaslónak számított, nem mérhető össze a szövetséges csapatok hagyományos gyalogságával sem, felszerelésük minősége és mennyisége jóval alatta marad avelük szemben álló Szövetséges csapatokénál.

[13] Február 13-án amerikai gépek lebombáztak egy iraki gyermektápszer-üzemet, amelynek rendeltetéséről ellenmondásos hírek érkeztek. A Vezérkari Főnökök Egyesített Tanácsának elnöke, Colin Powell azt állította, hogy az üzemben biológiai fegyvereket állítanak elő. Később kiderült, a lakosok óvóhelyként használták, így a bombázások legalább 315 embert öltek meg, köztük 130 gyermeket. Eközben Huszein továbbfolytatta az iraki és kuvaiti lakosok élőpajzsként való alkalmazását gyárak és katonai létesítmények körül.

A szövetségesek a vadász-, vadászbombázó repülőgépek és csatarepülőgépek, sőt harci helikopterek és hadászat B-52-es bombázó repülőgépek támogatásával, négynapos harctevékenységgel felszámolták az iraki csoportosítást, majd közvetlenül a szárazföldi hadművelet megindítása előtt végrehajtották a Második Világháború óta legnagyobb légideszant hadműveletet.

A harmadik időszak eseményei a következők voltak: 1991. február 24-28. között a szövetségesek megőrizték a légi fölényt és elszigetelték a harcmezőket. A kuvaiti hadműveleti csoportosítás és a Köztársasági Gárda fő erői szétzúzásának befejezése, az iraki erők és a katonai vezetési rendszer Észak-Irak területére való átmentésének megakadályozása volt a következő stratégiai lépés. A szövetséges csapatok több helyen kezdték meg az inváziót a szaúdi határon, a Bászrát Kuvaittal összekötő autópályát pedig lezárták, hogy elvágják az iraki hadsereg utánpótlását. A támadásban szaúdiak is részt vettek. A szövetségesek lebombázták az autópályán menekülő páncélosokat, amelyben több ezer ember vesztette életét, ezért ez a hely a „halál sztrádájaként”[14] vált ismertté. A visszavonuló irakiak több száz olajkutat gyújtottak fel.

A légi hadjárat magában foglalta a hadászati, harcászati és a haditengerészeti légierőnek hagyományos fedélzeti pusztító eszközökkel, valamint repülőgép - és hajófedélzeti manőverező robotrepülőgépekkel mért nagy mélységű olyan csapásait.

A törökországi repülőcsoportosítást az Irak központi körzetei felé vezető, déli légi hadműveleti irányban vezették be.

A támadó szárazföldi csapatok légi támogatását az ún. Harcászati Légierő Parancsnokság vezette.

Az USA légierő több tízezer tonna bombát dobott le és több ezer tonna kisebb lövedékeket használt el. A szövetségesek vesztesége az egyes bevetéseknél prognosztizált 3% helyett a légi tevékenységek teljes időszakára kivetítve nem érte el a 0,04% -ot!

1991. január 18-ától február 25-ig közel száz hadműveleti-harcászati rakétát indítottak Szaúd-Arábia és Izrael[15] területére[16]. A szövetségesek ezt háromlépcsős rakétavédelmi rendszer kiépítésével és üzemeltetésével igyekeztek kivédeni.

Az indított SCUD rakéták hatása jelentéktelen volt, azonban egy ellenséges izraeli válaszcsapás az Irak-ellenes koalíció felbomlásához és a háború Izraelre való kiterjedéséhez vezethetett volna. Irak elnöke feltehetően ezt szerette volna kiprovokálni. Ekkor kerültek először bevetésre a "Patriot" rakétaelhárító komplexumok[17].

Miután Szaddam Husszein[18] Bush elnöknek 1991. február 23-én tett utolsó felszólítás ellenére sem kezdte meg kivonulását Kuvaitból, megkezdődött az Öbölháború utolsó szakasza, "Sivatag Kard"[19] fedőnévvel. A szárazföldi hadművelet megindulásának időpontjára az iraki légierő[20] harcképtelenné vált.

A Perzsa-öböl felöl a kuvaiti partok közelében Missouri csatahajók[21] a part menti sávra kilőtt tömeges tűzcsapásaival és a partraszállás imitálásával megtévesztő manővert hajtottak

---

[14] http://hu.wikipedia.org/wiki/%C3%96b%C3%B6lh%C3%A1bor%C3%BA (letöltve: 2012-02-05)

[15] http://hu.wikipedia.org/wiki/%C3%96b%C3%B6lh%C3%A1bor%C3%BA (letöltve: 2012-02-05)

16 Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 18. oldal

[17] http://www.army-technology.com/projects/patriot/ (letöltve: 2012-02-05)

18 Szaddám Huszein Abd el-Madzsíd et-Tikríti[1] (arabul صدام حسين عبد المجيد التكريتي; el-Audzsa, 1937. április 28.[2] – Kázimajn, 2006. december 30.) iraki elnök, diktátor. Elnökként azt kívánta elérni, hogy Irak a Közép-Kelet egyik vezető állama legyen, ezért háborút vívott Iránnal. Saját hazájának bíróság 2006 novemberében ítélte akasztás általi halálra Szaddám Huszeint az 1982-es, 148 halálos áldozatot követelő dudzsaili mészárlás miatt. A volt iraki diktátort 2006. december 30-án végezték ki.

19 Az USA a Sivatagi Pajzs művelet keretében csapatokat telepített a veszélyeztetett Szaúd-Arábiába, ezt a műveletet 1990. november 8-án a támadóbb színezetű Sivatagi Kard váltotta fel.

20 Dr. Csabai György CSs: Visszatekintés az 1990-1991-es Öböl-háború tapasztalataira (letöltve: 2012-02-05)

[21] http://en.wikipedia.org/wiki/Gulf_War (letöltve: 2012-02-12)

végre. De Schwarzkopf nem innen hajtotta végre a fő hadművelet, hanem az ellenkező irányból[22]...

Az átkaroló csapásokat három fő irányba[23] mérték.

Az elsőt több tengerészgyalogos-hadosztály és egy páncélos hadosztály mérte északi, illetve észak-nyugati irányban.

A másodikat a 7. amerikai hadtest és a 18. légideszant-hadtest főerői és brit-francia csapatok mérték a szaúdi-kuvaiti-iraki hármas határtól nyugatra lévő határszakaszról északi irányban abból a célból, hogy fő erőikkel Kuvaitot északról megkerülve Bászra irányába mért csapással végleg megsemmisítsék a Köztársasági Gárda erőit. Az Eufrátesz völgyébe kijutva szándékoztak megsemmisíteni az iraki hadműveleti tartalékot, másrészről pedig a Kuvaitban lévő iraki erők utánpótlását elvágni és fő erőit bekerítve megsemmisíteni azt.

Az átkaroló hadművelet harmadik része egy megtévesztő manőver volt délről, főleg arab szövetséges erőkkel. Az ebben az irányban zajló harctevékenységek folyamán szenvedték a szövetségesek legnagyobb veszteségeiket, mert az irakiak pusztító aknavetőtűzzel árasztották el a térséget. A szárazföldi tevékenységet igen erős légi támogatás kísérte.

Február 28-án 5:00-kor, miután Szaddam Husszein hajlandó volt feltételek nélkül teljesíteni a Biztonsági Tanács határozataiba foglaltakat, Bush elnök tűzszünetet[24] rendelt el.

A Pentagon[25] hivatalos közleményei szerint a háború folyamán iraki részről megsemmisült 3 000 iraki harckocsi és 29 (!) hadosztály[26].

A háború többek között ezekkel a következményekkel zárult:

- Irak feltétel nélkül teljesítette az ENSZ határozatait
- A térségben az USA befolyása tovább erősödött
- És távolabbi következménynek értékelem azt, hogy az Iraki kurdok most látták meg a fegyveres harc kiújításához a megfelelő alkalmat.

IRODALOMJEGYZÉK

[1] John Keegan: Az iraki háború (Európa Könyvkiadó, 2004)

[2] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest)

[3] Magyar Hadtudományi Társaság: Hadtudományi Lexikon (Akadémiai Kiadó, 1995)

[4] Weiszhár Attila – Weiszhár Balázs: Háborúk lexikonja (Atheneaum Kiadó, Budapest 2004.)

[5] Dr. Csabai György CSs: Visszatekintés az 1990-1991-es Öböl-háború tapasztalataira

[6] Dr. Horváth Csaba: Az 1945 utáni legjelentősebb helyi háborúk és azok tapasztalatai (Zrínyi Miklós Nemzetvédelmi Egyetem nyomdája, 1999)

[7] Nagy Károly: Nemzetközi jog (Püski, Budapest, 1999)

[22] http://en.wikipedia.org/wiki/Gulf_War (letöltve: 2012-02-12)

[23] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 18. oldal

[24] 1991. február 28-án - közép-európai idő szerint reggel 6 órakor - írta alá George Bush amerikai elnök az Irak elleni háborúnak véget vető tűzszüneti rendelkezést.

[25] Az Amerikai Védelmi Minisztérium székhelye, Virginia állam Arlington megyéjében. Az amerikai hadsereg jelképe. A Pentagon névvel magát a minisztériumot illetik.

[26] Amaczi Viktor - Bombay László – Héjja István: A világ hadseregei (Zrínyi Kiadó, Budapest) 19. oldal

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Ferencz Bernadette - Vágföldi Zoltán
ferenczb@npp.hu - vagfoldi@hotmail.com

NATO 2ND SAMPLING AND IDENTIFICATION OF RADIOLOGICAL AGENTS LABORATORY PROFICIENCY TEST RESULTS (SIRA-2008)

Absztrakt/Abstract

Az alább cikkünkben áttekintést adunk az Észak-atlanti Szerződés tagállamainak 2008. évi radiológiai összemérési gyakorlatáról (2008 NATO Sampling and Identification of Radiological Agents II. Laboratory Exercise), ismertetjük annak célját és a mérési eredményeket, a megszerzett tapasztalatokat. Az összemérési gyakorlaton 13 NATO tagország 14 honvédségi/védelmi céllal fenntartott laboratórium vett részt – a szervező „Institute of Technology La Maranosa" Spanyol laboratóriumot is beleértve - a NATO/LG7/SIBCRA munkacsoport égisze alatt. Magyarországot a Magyar Honvédség Radiológiai Laboratóriuma képviselte, szakmai tanácsadóként és a mérések elvégzésében a Paksi Atomerőmű Zrt. és a Mezőgazdasági Szakigazgatási Hivatal Központ Radioanalitikai Referencia Laboratóriuma is részt vett.

This article demonstrates the results and experiences of the 2008 radiological laboratory exercise of the Party States of the 2nd North Atlantic Treaty Organization Sampling and Identification of Radiological Agents (NATO SIRA-2008) laboratory exercise. On this measurement exercise 14 defence dedicated laboratories of 13 NATO member countries – including the organizing institute "Institute of Technology La Maranosa" (ITM, Madrid, Spain) – took part, with the support of the NATO/LG7[1]/SIBCRA[2] working group. The Hungary was represented by the Hungarian Defence Forces Radiological Laboratory, with the Paks Nuclear Power Plant Radioanalytical Laboratory and the Agricultural Management Bureau Centre's Reference Laboratory for Radioanalysis acting as technical advisor and providing control measurements.

Kulcsszavak/Keywords: *SIRA gyakorlat, radionuklid azonosítás, gamma-spektrometria, alfa- spektrometria ~ SIRA exercise, radionuclide identification, gamma spectrometry, alpha spectrometry*

[1] LG/7: Land Group 7 on Joint NBC Defence (NATO workgroup)
[2] SIBCRA: Sampling and Identification of Biological, Chemical, and Radiological Agents (standardized procedure for sampling and identification procedures of CBRN agents according to AEP-66 NATO Handbook)

INTRODUCTION

The aim of this SIRA laboratory exercise was to compare the preparedness and capabilities of the NATO member countries' laboratories, preparing them for a possible "live" radiological or nuclear emergency or threat. The other aim of the comparison was also to prove the preparedness and performance of the participating laboratories (presented in Table 1) in the case of a given examination or measurement. This exercise continues the aim of 1st SIRA exercise. [1] It was based on a radiological transport accident and the analysis of an unknown long term stable radioactive liquid sample. A SIRA[3] is a NATO description of in situ survey, sampling and analysis. [2] After receiving the sample the laboratories have to report the description of radio analytical method, detected radioisotopes and their concentrations. According to the final result the laboratories give advice to incident commander or decision maker to manage hazardous situation.

RESULTS

A radiological scenario was simulated, and some laboratories have demonstrated being ready to produce a quick and accurate answer and radio analysis result. The scenario was a crash by a plane carrying a thermonuclear bomb, with no nuclear explosion occurring, but the bomb produced contamination when tactical explosives dispersed the radioactive charge. The scenario was a simulation of a real situation that happened in the past. A selection of radioisotopes from those that were present in the bomb, was made according to principal pollutants were present in a real case after the crash. In the Table 1 we present the participating laboratories.

N°	**Country**	**Participating Laboratories**	**Short name**
1.	Canada	Defence Research&Development	Def. R&D
2.	Czech Republic	NBC Defence Institute	NBC DI
3.	France	SPRA	SPRA
4.	Germany	Deployable NBC Analytical Laboratory	Deployable NBC AL
5.	Hungary	HDF Radiological Laboratory	HDF RL
6.	Italy	Centro Tecnico Logistico Interforze (Nuclear, Biological, Chemical)	CT Logistical Interforce NBC
7.	Netherlands	Organization for the Prohibition of Chemical Weapons	OPCW Laboratory
8.	Norway	Norwegian Defence Research Establishment FFI	Def. Res. Estab. FFI
9.	Poland	Military Institute of Chemistry and Radiometry	MI of Chem. and Radiometry
10.	Slovakia	RCBO Reference Chemical and Radiological Laboratory	Ref. Chem. and Rad. Lab.
11.	Spain (organizer)	Institut Technologico "La Maranosa"	ITM
12.	Sweden	Swedish Defence Research Agency	FOI
13.	United Kingdom	Atomic Weapons Establishment	AWE
14.	United Kingdom	Defence Science and Technology Lab.	DSTL

1. table. List of participating laboratories

The task of the participants was to identify radionuclides in the approx. 500 ml of material sample provided by the organizer laboratory (ITM, Madrid, Spain), both in quantity and quality.

[3] SIRA: Samling and Identification of Radiological Agents

Sample was prepared by organized spiking the total volume of ultra pure water ("Milli-Q" quality) acidified with ultra pure HNO_3 (analysis quality as stabilizer) with aliquots of weighed standards. After homogenization sub-samples were taken to test the sample homogeneity by liquid scintillation counter (LSC). Samples (Table 2) were prepared with the aim to allow the laboratories measure in a similar geometry to 500 ml Marinelli in a plastic container.

In the postage box we received all the needed information to participate in the exercise (sample description, the exercise written instructions and scenario).

According to the exercise rules the primary results were to be sent to the organizer within 24 hours of receipt via e-mail, with confirming radio analytical results to follow within a week, also via e-mail for a fast information exchange. The Hungary was represented by the Hungarian Defence Forces Radiological Laboratory (HDF RL), with the Paks Nuclear Power Plant (PNPP) and the Agricultural Management Bureau Centre's Reference Laboratory for Radio analysis (AMBC RLR) acting as technical advisor and providing control measurements.

The organizing laboratory after the laboratory test reported the liquid sample content, which contained two radionuclides. The participating laboratories (with different anonym laboratory codes A-N) located the Am-241 isotope with gamma spectrometric measuring system with semiconducting detectors and the Pu-239 activity with alpha spectroscopy.

The reference activity of the sample was 3.94 ± 0.16 Bq/kg in case of the Am-241 radioisotope. In view of the 24 hour measurement results only 5 of 13 laboratories reached the given ± 10% (± 0.39 Bq/kg) criteria, while in view of the week long measurements this figure was 7 of 13 (Figure 1 and 2).

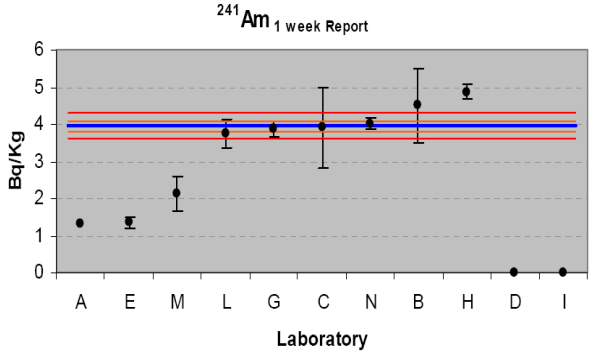


Figure 1.: Am-241 24 hrs. results (op. time)

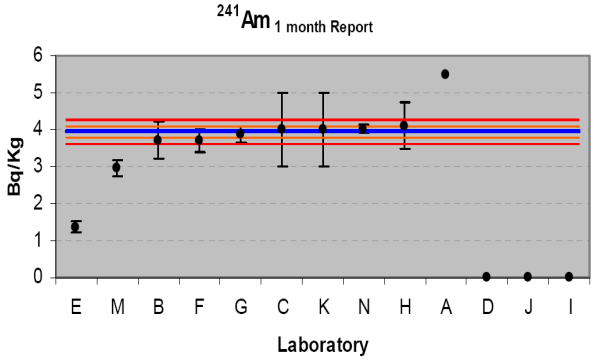


Figure 2. Am-241 1 week results (op. time)

Note: Hungarian Defence Forces Radiological Laboratory (HDF RL) code was K.

The activity of the Pu-239 (0.1% Pu-240 contamination) was 15.47 ± 0.72 Bq/kg. In 2 laboratories, the results of the 24 hour measurements were up to the stringent requirements of the ± 10% (± 1.55 Bq/kg), the number for the week long measurements was barely 3 (Figure 3 and 4).

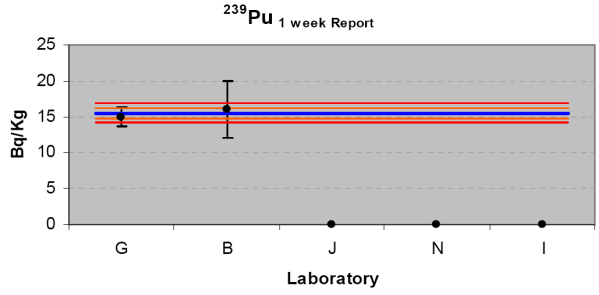


Figure 3. Pu-239 24 hrs. results (op. time)

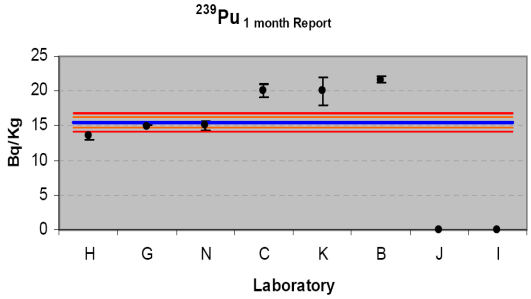


Figure 4. Pu-239 1 week results (op. time)

The identification and quantification of the Am-241 was made correctly by most of the participants. The identification of Pu-239 presented a higher difficulty for the laboratories, 3 laboratories had shown a perfect result in the identification and quantification.

In the Table 2 below we present the reported results by participating laboratories. The results have been normalized to Bq/kg units. Density of sample employed to normalize result from Bq/l to Bq/kg was 1.094 ± 0.001 kg/l.

Sample number/Lab. code	**24 h Report (Normalized Result)**		**1 Month Report (Normalized Result)**	
	Detected isotopes	**Certified Activity** [Bq/kg]	**Detected isotopes**	**Certified Activity** [Bq/kg]
08257/A	Am-241	1.3	Am-241	5.46
08257/B	Am-241 Pu-239	4.5±1.0 16±4	Am-241 Pu-239	3.7±0.5 21.6±0.5
08257/D	Am-241	Qualitative	Am-241	Qualitative
08257/E	Am-241	1.36±0.15	Am-241	1.36±0.15
08257/F	none		Am-241	3.7±0.3
08257/G	Am-241 Pu-239+Pu-240	3.88±0.21 15.0±1.3	Am-241 Pu-239+Pu-240	3.88±0.21 14.9±0.2
08257/H	Am-241	4.87±0.21	Am-241 Pu-239	4.1±0.62 13.5±0.54
08257/I	Pu-239 Am-241	Qualitative Qualitative	Pu-239 Am-241	Qualitative Qualitative
Sample number/Lab. code	**24 h Report (Normalized Result)**	**1 Month Report (Normalized Result)**	**Sample number/Lab. code**	**24 h Report (Normalized Result)**
08257/J	Pu-239	Qualitative	Pu-239 Am-241	Qualitative Qualitative
08257/K	none		Am-241 Pu-239	4±1 20±2
08257/L	Am-241	3.74±0.38	No participation	
08257/M	Am-241	2.13±0.45	Am-241	2.96±0.21
08257/N	Am-241 Pu-239+Pu-240	4.01±0.14 Qualitative	Am-241 Pu-239+Pu-240	4.01±0.11 15.0±0.6

Note: the Hungarian laboratory code (HDF RL) was K.

Table 2. Radioanalytical normalized results (cont.)

The results of this exercise according to Table 2 results shown a high heterogeneity between NATO radiological laboratories in resources, capabilities and working experience. In Table 3 we summarize the alpha and gamma spectrometry measuring conditions, method and equipment, which used the Hungarian laboratory.

Laboratory short name	Methods and equipments	
	Alpha spectrometry	**Gamma spectrometry**
HDF RL (K)	No equipment available*	Sample preparation: none Spectrometer: Canberra GC2020 coax. HpGe Geometry: 500 ml Marinelli, Pb shielding Measuring time: 24 h Analyzer: Inspector2000 Software: Genie2000 *Result:* Am-241 detected
AMBC RLR	Sample preparation: 10,00 cm^3 sample evaporation Spectrometer: Canberra Software: Canberra Apex Alpha Measuring time: 12 h Result: Am-241 and Pu-239	Sample preparation: none Spectrometer: Canberra HpGe Geometry: 500 ml Marinelli, Canberra Pb shielding Measuring time: 33,33 h Software: Winner 6.0 (FAST ComTec GmbH) *Result:* Am-241 detected
Laboratory short name	**Alpha spectrometry**	**Gamma spectrometry**
PNPP CES	Sample preparation: 4,00 cm^3 sample evaporation Spectrometer: Alpha Analyst M7200-04, 8 chambers Software: Canberra Apex Alpha Measuring time: 12 h Result: Am-241 and Pu-239	Sample preparation: none Spectrometer: Canberra HpGe Geometry: 10 ml plastic container Measuring time: 8,33 h Software: Canberra APEX Result: Below the detection limit

Table 3. Hungarian sample preparation, conditions and equipment (1 week) (cont.)

Abbreviations to Table 3:

HDF RL: Hungarian Defence Forces Radiological Laboratory

PNPP CES: Paks Nuclear Power Plant Operations Division, Chemical Engineering Section

AMBC RLR: Agricultural Management Bureau Center's Reference Laboratory for Radio analysis

In a Table 4 we present the three Hungarian laboratory control measurement results.

Nuclide	**ITM standard** [Bq/kg]	**HDF RL** [Bq/kg]	**AMBC RLR** [Bq/kg]	**PNPP CES** [Bq/kg]
Am-241	3,94 ± 0,16	4,0 ± 1	3,8 ± 0,2	3,66 ± 0,46
Pu-239 (Pu-239 + Pu-240)	15,47 ± 0,72	AMBC RLR result	20,1 ± 2,0	17,8 ± 1

Table 4. Hungarian radioanalytical results

*Note: HDF Radiological Laboratory doesn't have a liquid scintillation counter, for Pu-239 we presented the AMBC RLR results and figures.

Events show, that in spite of the different instruments and methods of measurement, within the results of the three Hungarian laboratories, with scatter adjustment, are whithin the reference values published by the organising laboratory.

The organizer did the evaluation of the laboratories' results according to the ISO 13528 (2005) and ISO/IEC 43 guide (1997) the accepted limits of the measurements were ±10 % of the actual value.

Main statistic proposed:

U-score/E_n numbers: $$E_n = \frac{x - X}{\sqrt{u_x^2 + U_x^2}}$$

Where:
x: reported value of participant laboratory,
X: assigned value determined in a reference laboratory,
U_x: expanded uncertainty of X,
u_x: expanded uncertainty of a participant's result.

u-score acceptance criteria: unsatisfactory $|u| > 2.58$
satisfactory $|u| < 2.58$

U-score								
Laboratory code	**24 hours (operational time)**				**1 week (operational time)**			
	Am-241		**Pu-239**		**Am-241**		**Pu-239**	
A(1)	Det.				Det.			
B(2)	0.19	**< 2.58**	0.23	**< 2.58**	0.46	**< 2.58**	7.00	**> 2.58**
C(3)	0.36	**< 2.58**			0.31	**< 2.58**	2.41	**< 2.58**
D(4)	Det.				Det.			
E(5)	12.7	**> 2.58**			12.7	**> 2.58**		
F(6)					1.75	**< 2.58**		
G(7)	0.23	**< 2.58**	0.32	**< 2.58**	0.23	**< 2.58**	0.78	**< 2.58**
H(8)	3.5	**> 2.58**			0.25	**< 2.58**	2.20	**< 2.58**
I(9)	Det.		Det.		Det.		Det.	
J(10)			Det.		Det.		Det.	
K(11)					0.06	**< 2.58**	2.13	**< 2.58**
L(12)	1.36	**< 2.58**						
M(13)	4.51	**> 2.58**			4.92	**> 2.58**		
N(14)	0.32	**< 2.58**	Det.		0.35	**< 2.58**	0.33	**< 2.58**

Table 5. U-score results

Legend and comments: "Det": "Detected" the participant has reported the isotope qualitative, but he has not given an estimation of uncertainty that allows U-score calculus. Light grey: no data, dark grey: outside the accepted value (unsatisfactory, $u > 2.58$), diagonal striped: Satisfactory measured result ($u < 2.58$)

The participation of this proficiency test exercise was very useful for all laboratories to test laboratory capabilities and compare the results. We planned to participate in the future on the next NATO SIRA exercise.

CONCLUSION

Most of the participating laboratories were successful in completing the measurement exercise and taking part in the SIRA-2008 exercise. Spectrometric identification of the Am-241 gamma did not pose much of a problem for most of the laboratories. Based on the 24 hour measurement results of the Pu-239 alpha spectrometric identification, altogether two laboratories were successful, based on the one week measurement results, three laboratories were fully within the acceptance criteria (measurement time could be increased). Knowing the low alpha activity concentration of the sample the primarily communicated results are acceptable, since the organizers gave extremely strict acceptability criteria.

The main reason for the failure was that the laboratories did not publish results of the measurements, did not publish standard deviation or that their results were outside the stringent ± 10% limit. In samples of small concentration of alpha radiating activity (below 20 Bq/kg) we consider a larger margin (± 25%) to be acceptable. Most of the participating laboratories were well equipped, but HDF RL not equipped with alpha spectrometer. In the future the main task is to develop technical and human resources in HDF RL according to SIRA Handbook (AEP-49) recommendations. [3]

ACKNOWLEDGEMENTS

We wish to acknowledge the result and the contributions of organizing and participating laboratories in the SIRA exercise: Raul Lopez S (ITM "La Maranosa", Spain), Elizabeth Inrig (Defence R&D, Canada), Petr Sladek (NBC Defence Institute, Czech Republic, N. Chianea (SPRA, France), M. Kitto (Deployable NBC Analytical Laboratory, Germany), A. MAssaro ()entro Tecnico Logistico Interforze NBC, Italy), Gary Mallard (OPCW Laboratory, The Netherlands), B. Hanne (Norwegian Defence Research Establishment FFI, Norway), M. Ceremuga (Military Institute of Chemistry and Radiometry, Poland), K. Lizon (RCBO Reference Chemical Laboratory, Slovakia), T. Annika (FOI, Sweden), M. Simpson (DSTL, United Kingdom), T. Paul (AWE, United Kingdom), S. Tarján (AMBC RLR, Hungary),

REFERENCES

[1] Haslip, Dean S.; Mercier, J. R.: A NATO Exercise on Radiological Sampling, Health Physics, November 2004, Volume 87, pp. S63-S67

[2] NATO AEP-49 Sampling and Identification of Radiological Agents (SIRA) Handbook, 2004, (NATO/PfP Unclassified)

[3] Raul Lopez S.: 2008 NATO SIRA Laboratory Exercise Technical Report, La Maranosa, Spain, 2009 (NATO/PfP Unclassified)

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Muha Lajos
muha.lajos@uni-nke.hu

FORMÁLIS BIZTONSÁGI MODELLEK I.
A DISZKRECIONÁLIS HOZZÁFÉRÉS-VÉDELEM

Absztrakt

A biztonságos informatikai rendszerek megteremtésére irányuló erőfeszítések folyamatosak. A nagy biztonságú informatikai rendszerek esetében alapvető követelmény a biztonság formális leírása és bizonyítása. Ezért már az informatikai biztonság kezdetétől számos formális modellt dolgoztak ki a biztonsági elvárások leírására és bizonyítására. Ez a cikksorozat ezeket a formális modelleket kívánja bemutatni, és felhasználhatóságuk szempontjából összehasonlítani. Jelen a cikk a hozzáférés-vezérlés elveit és alapvető eljárásait írja le.

Efforts to build secure computer systems are continuous. The formally description and verification of security is a fundamental requirement of the high-security information systems. Therefore, many formal models have been developed to describe and verification of security requirements. This article series aims to present them and their comparison, based on the usability. This article reviews basic principles and procedures of the access control.

Kulcsszavak: *informatikai biztonság, adatvédelem, bizalmasság, sértetlenség, formális modell, hozzáférés-ellenőrzés, biztonsági osztályok ~ information security, privacy, confidentiality, integrity, formal model, access control, security classes*

1. BEVEZETÉS

Az informatikai rendszerek biztonsága terén már az 1970-es évek elején felmerült az információvédelem formális meghatározásának, mint biztonságpolitikának, illetve e biztonságpolitika betartásának formális úton történő ellenőrzésének igénye. Ennek az igénynek a megvalósítására azóta számos mű (Bell-LaPadula modell [1], Biba modell [2], Clar-Wilson modell [3], stb.) született, amelyek az információvédelem kapcsán leírják [4]:

1. A biztonság formális meghatározását.
2. Az alanyok jogosultságainak meghatározását objektumokhoz és más alanyokhoz.
3. Az információ védelemmel kapcsolatos alapvető tulajdonságainak (bizalmasság, sértetlenség, elérhetőség, elszámoltathatóság) meghatározását,
4. Az adatokhoz való hozzáférés megoldási módjait.
5. Formális modellek felépítését az adatok védelme alábbi kérdéseinek vizsgálatához:
   - a bizalmasság biztosítása,
   - a sértetlenség biztosítása,
   - a jogosulatlan jogosultság áramlás (szivárgás),
   - a „biztonságos” adatáramlás biztosítása.
6. A formális modellek vizsgálatának eredményeit – az adatok megfelelő védelmét biztosító szabályok megfogalmazását.
7. A formális mechanizmusok (mátrixok, rácsok, gráfok) felhasználását az adatokhoz való hozzáférés megoldási módjainak, és azok áramlásának leírásához.

Ebben a cikkben a fentiek közül az adatok védelmére alkotott formális modellek ismertetése mellett azok összevetését, és a felhasználási lehetőségeiket szeretném bemutatni.

2. ALAPFOGALMAK

A cikk a következő fogalmakat használja:

- Biztonság,
  Információvédelem: Ebben a cikkben a NATO INFOSEC meghatározását veszem alapul: „a biztonsági rendszabályok alkalmazása a kommunikációs, információs és más elektronikus rendszerekben a feldolgozott, tárolt vagy továbbított információ bizalmasságának, sértetlenségének vagy rendelkezésre állásának véletlen vagy szándékos elvesztése ellen, és e rendszerek sértetlenségének vagy rendelkezésre állásának elvesztése ellen”. [5].
- Formális – informális – szemiformális [6]:
  - Informális leírás: valamilyen természetes nyelven készült leírás.
  - Szemiformális leírás: szabályelvű természetes nyelven készült leírás, pl. strukturált tervezési módszereknél használt adatfolyam, entitás-reláció, állapot-átmenet, stb.
  - Formális leírás: szintaktikusan és szemantikusan szabályozott specifikációs (formális) nyelven, tipikusan a matematikai logika nyelvén készült leírás.
  - Formális bizonyítás: Formális nyelven, levezetési szabályokkal és módszerekkel történő bizonyítás,
  - Formális biztonságpolitikai modell: formális nyelven leírt biztonsági politika modell;
- Alanyok (S-subjects): aktív entitások[1];
- Objektumok (O-objects): passzív entitások[2];

[1] felhasználók, akik az alkalmazásaikkal fenyegetést jelenthetnek.
[2] az adatok kezelését végző egységek (fájlok, könyvtárak, programok, stb.) – védelem alatt állnak.

- Hozzáférés-vezérlés (Access Control): "Az erőforrás jogosulatlan használatának megelőzése, beleértve erőforrás jogosulatlan módon való használatának a megelőzését" [7];
- Hozzáférési mód (Acces Method): az objektumokhoz való hozzáférés lehetősége, az adatáramlás iránya;
- Szabályok (Rules): a hozzáférés-vezérlés módjának meghatározása.
- Jogosultságok (Permissions): az objektumokon végrehajtandó tevékenységek végrehajtásának lehetősége (joga);
- Feljogosítás (Authorization): az alanyoknak az objektumok feletti jogosultságok megadása és felügyelete;
- Axiómák (Axioms): tulajdonságok, amelyeket a rendszernek teljesíteni kell, hogy az adott biztonsági modellben biztonságosnak fogadjuk el;
- Predikátumok (Predicates): annak meghatározására szolgálnak, hogy az alanynak van-e jogosultsága az objektumon, értéke lehet igaz (true) vagy hamis (false);
- Katonai biztonsági modell (Military Security Model): a minősített adatokat (szigoruan titkos, titkos, bizalmas, ...) tartalmazó (nem csak katonai!) rendszerekre vonatkozó modellek csoportja;
- Üzleti biztonsági modell (Business Security Model): a nem minősített adatokat (kiemelt jelentőségű, üzleti titok, nyílt) tartalmazó rendszerekre vonatkozó modellek csoportja.

3. A KLASSZIKUS HOZZÁFÉRÉS-VEZÉRLÉSEK ALAPJAI

A formális biztonsági modellek különböző hozzáférés-vezérléseken alapulnak. Ezeket a hozzáférés-védelem kialakítása során – formális biztonsági modellben való felhasználás nélkül is – alkalmazzák. Számtalan módosított, továbbfejlesztett változatuk létezik, itt csak a klasszikusnak nevezhető változataik kerülnek bemutatásra.

3.1. Az NTK szabály

A hozzáférés-vezérlések jelentős része a közismert *kell, hogy tudja*[3] elven alapul. A *kell, hogy tudja* elv azt jelenti, hogy egy adathoz (információhoz) csak az kaphat hozzáférési engedélyt, akinek adott információt a feladatköre miatt szükséges hozzáférnie (szükséges és elégséges jogosultság).

Az NTK szabály abból a feltételezésből indul ki, hogy minden objektum legalább egy adattárolóval (angolul container) kapcsolatban áll, *Container(O)* az *O* objektummal kapcsolatban álló adattárolók halmaza. *NTK(S)* az *S* alany által elérhető adattárolók halmaza. A biztonságpolitika a következő szabályokat valósítja meg:

Az *S* alany hozzáférhet az O objektumhoz, ha:

Container(O) $\subseteq$ *NTK(S)* (ha az *O* objektum minden tárolójához hozzáférhet az *S* alany).

A módosított NTK szabály

Az NTK szabály módosítása figyelembe veszi az adatáramlás irányát (írás, olvasás) is.

S alany olvasási joggal hozzáférhet O objektumhoz, ha:

Container(O) $\subseteq$ *NTK(S)* (ha az *O* objektum minden tárolójához hozzáférhet az *S* alany).

S alany írási joggal hozzáférhet O objektumhoz, ha:

Container(O) $\supseteq$ *NTK(S)* (ha az *S* alany csak az *O* objektum tárolóihoz férhet hozzá).

[3] Need to know

Nézzünk egy példát:

A rendszerben található adattárolók: {céges adatok – *B*, pénzügyi adatok – *F*, személyes adatok – *P*, egészségügyi adatok - *M*},

Container(O) = {M, F}

$NTK(S_1)=\{F\}$, vagyis az S_1 alanynak csak a pénzügyi adatokhoz (*F*) van hozzáférése, ezért S_1 alany írhat *O* objektumba,

$NTK(S_2)=\{P\}$, vagyis az S_2 alanynak az egészségügyi és a pénzügyi adatokhoz (*M, F*) nincs hozzáférése, ezért S_2 alanynak nincs semmilyen hozzáférése az *O* objektumhoz,

$NTK(S_3)=\{C, F\}$, vagyis az S_3 alanynak a pénzügyi adatokon (*F*) kívül a céges adatokhoz (*B*) is hozzáférése van, de az egészségügyi nincs hozzáférése, ezért S_3 alanynak nincs semmilyen hozzáférése az *O* objektumhoz,

$NTK(S_4)=\{P, M\}$, vagyis az S_4 alanynak az egészségügyi adatokon (*M*) kívül a személyes adatokhoz (*P*) is hozzáférése van, de a pénzügyi adatokhoz (*F*) nincs hozzáférése, ezért S_4 alanynak nincs semmilyen hozzáférése az *O* objektumhoz,

$NTK(S_5)=\{F, M, P\}$, vagyis az S_5 alanynak hozzáférése van a pénzügyi és az egészségügyi adatokhoz (*M, F*) is, de ezenkívül a személyes adatokhoz (*P*) is, ezért S_5 alany olvashatja az *O* objektumot, de nem írhat bele.

3.2 Diszkrecionális hozzáférés-vezérlés

A diszkrecionális, vagyis szabad belátás szerint kialakított hozzáférés-vezérlés (röviden: DAC[4]), más néven mátrix modell, vagy jogosultságok táblázata az első hozzáférés-védelmi megoldás volt. A diszkrecionális hozzáférés-vezérlés az alapja az alanyok azonosítása. Az eljárást azért nevezik diszkrecionálisnak, mert legfontosabb jellemzője, hogy amennyiben egy alany rendelkezik egy objektumhoz valamilyen hozzáférési jogosultsággal, akkor ezt a jogosultságot szabad belátása szerint tovább adhatja más alanyoknak, vagyis ez a szabályozási mód az alanyoknak az objektumok feletti jogosultságok kiosztását jelenti. A DAC a gyakorlatban többnyire a közismert *hozzáférés-vezérlési lista* (röviden: ACL[5]) alkalmazásán alapul.

A DAC – bár szokás a formális modellek között emlegetni – valójában nem formális, hanem szemiformális modell, mivel leírása nem a matematikai logika nyelvén történik, hanem egy szabályelvű természetes nyelven készült entitás-reláció. A DAC megoldásának és alkalmazásának egyik első leírói G. Scott Graham és Peter J. Denning voltak a Protection – Principles and practice cikkükben [8]. A DAC alkalmazását az USA Védelemi Minisztérium kiadványa, a Narancs Könyv[6] [9] a C2 és a C1 biztonsági osztályokban írta elő kötelező tette. A Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság 12. számú ajánlása [10] az alapbiztonsági osztályban, majd a Közigazgatási Informatikai Bizottság 25. számú ajánlása 1-2. kötete az IBIK [11] a 0., 1. és 2. biztonsági szinteken előírta az alkalmazását.

A védelmi rendszer elemei [8]:

- *objektumok* (pl.: fájl könyvtár, stb.) halmaza;
- *alanyok* (felhasználók, illetve az általuk futtatott folyamatok) halmaza;

[4] Discretionary Access Control

[5] Access Control List

[6] A borítójának színéről Narancs Könyv (Orange Book) néven közismerté vált Trusted Computer System Evaluation Criteria (TCSEC, magyarul Biztonságos Számítógépes Rendszerek Értékelési Kritériumai) az Amerikai Egyesült Államok Védelmi Minisztériumának 1983-ban kiadott nyilvános informatikai biztonsági követelménygyűjteménye, amelynek alkalmazása az USA-ban majd 20 évig kötelező volt a kormányzati, katonai rendszerek vonatkozásában.

– *szabályok* az alanyoknak az objektumokhoz való hozzáférésének vezérléséhez

Az egyes objektumokhoz való hozzáférési jogot a alanyok számára az objektum tulajdonosa[7] (owner) állítja be. A hozzáférés-vezérlési listában implicit vagy explicit módon szerepel az objektum, az alany és az engedélyezett, illetve tiltott művelet. Kivétel nélkül minden hozzáférési kísérlet ellenőrzésre kerül.

Az alapvető hozzáférési műveletek:

– olvasás (read),
– írás (write),
– végrehajtás (execute).

A DAC megvalósítására tipikus példája a „klasszikus" UNIX operációs rendszer hozzáférés-védelmi megoldása. Ez egy egyszerű, de kevésbé rugalmas hozzáférés-védelmi rendszer, ahol csak az alapvető hozzáférési műveletek, az olvasás, az írás és a végrehajtás alkalmazhatóak.

Az alanyokat (felhasználókat) egyedi azonosítóval rendelkeznek és egy elsődleges, azonos védelmi szintű alanyok csoportjának tagja. Az alanyokat és az objektumokat egy (csoportszám, tagszám) párossal azonosítják, ahol az objektumok felveszik az őket létrehozó alany kódjait. Az objektum és ahhoz hozzáférni kívánó alany kódpárosa alapján az alany az alábbi három csoport valamelyikébe sorolható, és minden objektumnál e három csoportra vonatkozó jogosultságok szerepelnek:

- tulajdonos, ahol a csoportszám és a tagszám azonos,
- csoport, a csoportszám megegyezik,
- világ (mindenki a tulajdonoson, a tulajdonos csoportjának tagjain kívül), egyik kódszám sem egyezik meg.

A megvalósításhoz minden objektumhoz hozzárendelésre kerül egy 12 bites szó, amelyből 9 bit a hozzáférés-védelem leírása, ahol a hárombites csoportokban az olvasás, írás és a végrehajtási jogok szerepelnek. Például

rwx rw- ---

Az első három bit a tulajdonos olvasási, írási és végrehajtási jogát jelöli. A következő három bit a tulajdonos csoportja tagjainak olvasási és írási jogát jelöli. A tulajdonoson, a tulajdonos csoportjának tagjain kívüli felhasználóknak nincs semmilyen hozzáférési joga.

A hozzáférési mátrix a S_i alany által az O_j objektumon elvégezhető lehetséges $A(S_i, O_j)$ hozzáférési műveleteket jeleniti meg.

		OBJEKTUMOK						
		Alanyok			Fájlok		Eszközök	
		S_1	S_2	S_3	F_1	F_2	D_1	D_2
ALANYOK	S_1		block wakeup		Read write		seek	
	S_2			Stop		update		Seek
	S_3				Delete	execute		

1. ábra. Egy hozzáférési mátrix részlete [8]

[7] Az objektum tulajdonosa annak létrehozója, vagy akire átruházták ezt a tulajdonságot.

Az un. kiterjesztett hozzáférési mátrixban[8] megjelenik a tulajdonosi jog (owner) és a hozzáférés-vezérlést kezelő jog (control), valamint a *jogmásolás* lehetősége. A tulajdonosi jog az adott objektumon lehetővé teszi más alanyok hozzáférési jogainak kezelését. Tulajdonosa minden objektumnak csak egy lehet. A hozzáférés-vezérlést kezelő jog csak alanyok között értelmezett és lehetővé teszi más alanyok hozzáférési jogainak kezelését. Ahhoz, hogy egy adott objektumon valamely alany meglévő hozzáférési jogait átadhatóak legyen egy másik alanynak, bevezetésre került a jogmásolási, mint vezérlési lehetőség. A jogmásolás lehetőségét *-gal jelölik. A kiterjesztett hozzáférési mátrixban kívül rendszerenként eltérő hozzáférési műveleteket (módosítás, törlés, jogosultságkezelés, stb.) is megvalósítanak.

		OBJEKTUMOK						
		Alanyok			Fájlok		Eszközök	
		S_1	S_2	S_3	F_1	F_2	D_1	D_2
ALANYOK	S_1	control	owner block wakeup	owner control	read * write *		seek	Owner
	S_2		control	stop	Owner	update	owner	seek *
	S_3			Control	Delete	owner execute		

2. ábra. Egy kiterjesztett hozzáférési mátrix részlete [8]

A DAC használatához fel kell tételeznünk, hogy:

1. a felhasználók védik a saját információikat
2. a felhasználók megoszthatják jogosultságaikat a többi felhasználóval
3. a felhasználók meghatározhatják a másokhoz rendelt hozzáférési típusát.
4. a felhasználók felelősek a biztonságpolitikáért.

A diszkrecionális hozzáférés-vezérlést használja sok PC-s és hálózati operációs rendszer, így a MS Windows NT és a MS Windows 2000 operációs rendszer, számos hagyományos UNIX és LINUX operációs rendszer hozzáférés-védelme is a diszkrecionális hozzáférés-vezérlésen alapul. A nem nagy biztonságú adatbázis-kezelők is többnyire a diszkrecionális hozzáférés-vezérlést használják.

A DAC nagy hibája, hogy nem tudja garantálni az adatok bizalmasságát! Ha valakinek olvasási joga van egy objektumhoz, akkor ő már másolhatja is ezeket az adatokat a *copy/paste* segítségével. Sőt – mint azt többek között William Stallings és Lawrie Brown a Computer Security: Principles and Practice című könyvükben [12] bemutatják – egy alany az O_1 objektumon meglévő olvasási jogát kihasználva, egy un. trójai program segítségével az O_1 objektumban lévő információt képes elolvás után az O_2 objektumba kiírni, és ehhez olvasási jogot adni egy olyan alany részére is, akinek ez kifejezetten tilos volt.

A fenti szituáció elkerülésére hozták létre *a kötelező hozzáférés-vezérlési modelleket* (röviden MAC[9]). E modellek közös tulajdonsága, hogy nem az objektumokkal végezhető műveletekre, hanem az azokban tárolt információ áramlására fektetik a hangsúlyt.

[8] Extended access matrix

[9] Mandatory Access Control

IRODALOM

[1] D. Elliot BELL, Leonard J. LAPADULA: *Secure Computer Systems: Mathematical Foundations and Model*, Mitre Corporation, 1975.

[2] Kenneth J. BIBA: *Integrity Considerations for Secure Computer Systems,* Mitre TR-3153, Mitre Corporation, Bedford, Massachusetts, 1977.

[3] David D. CLARK and David R. WILSON: *A comparison of Commercial and Military Computer Security Policies*, in Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87), pp. 184–193, Oakland, CA, USA, 1987.

[4] Krzysztof LIDERMAN: *Podstawowe Twierdzenie Bezpieczeństwa*, Biuletyn Instytutu Automatyki i Robotyki WAT, pp. 85-102, Warszawa, 2011.

[5] *Security within the North Atlantic Treaty Organisation (NATO)* – C-M(2002)49, NATO, 2002.

[6] BODLAKI Ákos, MUHA Lajos: *Az informatikai biztonság tanúsítási és minősítési eljárásrendjének terve*, tanulmány a Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottság részére, Budapest, 1997.

[7] *ISO 7498-2:1989: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture*, International Organization for Standardization, 1989.

[8] G. Scott GRAHAM, Peter J. DENNING: *Protection – Principles and practice*, Joint Computer Conference 40, pp. 417-429, AFIPS Press, Montvale, N.J., USA, 1972.

[9] *Trusted Computer System Evaluation Criteria* – CSC-STD-001-83, Department of Defense, Washington D.C., 1983.

[10] BODLAKI Ákos, CSERNAY Andor, MÁTYÁS Péter, MUHA Lajos, PAPP György, VADÁSZ Dezső: *Informatikai rendszerek biztonsági követelményei*, Miniszterelnöki Hivatal, 1996.

[11] Déri Zoltán, Lobogós Katalin, Muha Lajos, Sneé Péter, Váncsa Julianna: *Informatikai Biztonság Irányítási Követelmények (IBIK)*, Miniszterelnöki Hivatal, Budapest, 2008.

[12] William STALLINGS, Lawrie BROWN: *Computer Security: Principles and Practice*, Prentice Hall Press Upper Saddle River, NJ, USA, 2007.

HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Alejandra Román Rodriguez - Barbarics Tamás
alejandra.roman.rodriguez@gmail.com - barbarics@evt.bme.hu

FOREIGN MILITARY BASES WITH RENEWABLE ENERGY SOURCES

Absztrakt/Abstract

Jelen írás azokat a megújuló energiaforrásokat mutatja be, amelyek külföldön telepített katonai bázisokon alkalmazhatóak. Az írás külön bemutatja az amerikai hadsereg ilyen irányú tevékenységét, mivel ennek elkötelezettsége a zöld források irányában igen komoly, valamint e hadsereg a megújuló energiáknak nagy szerepet szán a hadviselésben, illetve ez az az ország, amely a legtöbb erőt állomásoztatja külföldi országokban.

The paper discusses the advantages of the renewable energies applied in foreign military bases. In the paper the U.S. military is discussed because of their commitment to green sources, the alternatives that they are already developing related to the use of renewable energies in warfare, because they are at war, and finally because they are the country with the largest number of forces in foreign countries.

Kulcsszavak/keywords: *megújuló energiák, katonai, külföldi bázisok ~ renewable energies, military, foreign bases*

1. Introduction

The climate change, global warming and their causes and consequences are become more and more important, the politicians, nations, citizens, everyone is getting more concerned about them. There are initiatives in every single social level to try to stop this tendency. Many types of renewable energies can be used in ordinary buildings like houses or blocks of flats, and their installation is rather easy. The number of governments installing renewable energy power plants is increasing everywhere in the world. For many underdeveloped countries renewable energy provides them with a good solution for their energetic problems, eliminating the dependence on other countries, and being able to produce their own energy, an energy that is clean and that has much more stable costs over the long-term. Some of these green sources have been harnessed by humans for centuries. This is the case of solar, geothermal or wind energy, the difference is that now the way in which they are harnessed has improved and we can take more advantage of them.

The main goal of this paper is to discuss the advantages that the use of renewable energies can have for the military. The military force of U.S. is taken into account because of their commitment to green sources, the alternatives that they are already developing related to the use of renewable energies in warfare, because they are at war, and finally because they are the country with the largest number of forces abroad, for example in Afghanistan.

2. United States and the petroleum

Historically, energy has been treated in the U.S. as cheap commodity that was always available when it was needed. These facts may no longer be true, especially after the price escalation in 2008, the prospects that prices will rise as world oil reserves start to decrease, and the difficulties that resupply convoys have to face in war situations like Afghanistan. According to the most recent data on petroleum available at the U.S Energy Information Administration web page, the United States is the top oil consumer in the world, with a consumption that in 2008 represented 22.80 percent of the total petroleum consumption in the world [2, 3]. In 2008, the Department of Defense (DoD) spent more than $16 million to buy 120 million barrels of oil; this figure amounts to 1.7 percent of the total in the U.S, making it the single largest oil consumer in the United States [4]. According to this study on energy use in wartime from Second World War to the current Middle East wars, nowadays the U.S. fuel consumption is 83.3 liters per soldier and day. That figure represents a 175 percent increase in the fuel consumed by U.S. soldiers compared to the consumption in Vietnam per soldier and per day. This increase in fuel consumption is mainly due to the increasing number of different technologies with which soldiers are equipped nowadays, as well as the asymmetric nature of the conflicts, which take place in irregular situations where it is necessary to travel over long distances because there are not clearly defined fronts. In this type of conflicts, armies have to spread their forces as much as possible in order to protect as many assets as they can. This results in larger number of bases spread along long distances and in an increased number of convoys to supply them.

Afghanistan was selected as a target in this paper, because of the number of military forces present in the country, around 100,000 troops according to NATO [1] and around 70 percent of them are from the U.S. Because of the asymmetric nature of the conflict, which makes military forces to be spread all over the country, this results in an increased number of resupply convoys, and those convoys have to travel over long distances to reach their destinies. This is one of the reasons why the U.S. military decided to start using renewable energies in their bases abroad. Another reason has been the fact that the complete withdrawal

of all the forces in Afghanistan will still take years, so there is still time to apply some of the technologies that are being under consideration.

The increasing number of convoys is an important cause of casualties because they are a usual target for enemy forces, who try to disrupt friendly fighting forces energy supply by means of Improvised Explosive Devices (IEDs) and roadside bombs. The number of security incidents in Afghanistan has increased significantly when compared to previous years. They state that this situation is attributable to the increase in military operations that has been taking place since the first quarter of 2010, and also to the significant anti-government activities taking place in the south-east and eastern regions of Afghanistan. The report also points out that the majority of incidents continue to involve armed clashes and IEDs, each of them represents one third of the reported incidents. One of the most important issues in the report is the alarming increase of incidents related to IEDs, which have recorded a 94 percent increase in the first four months of 2010 compared to the same period in 2009. As well, they also report an increase in the number of suicide attacks and complex suicide attacks, which demonstrates the growing capability of the local terrorist networks linked to Al-Qaida. The 45 percent increase of the number of assassinations among civilian population when compared to the same period in 2009 is also significant. The current number of assassinated people per week is 7 [5].

The Army Environmental Police Institute (AEPI) calculated the casualty factor (casualties per convoy) for fuel and water resupply convoys in Afghanistan. The factors for fuel and water resupply are 0.042 and 0.034 respectively. The up-to-date data on casualties in Afghanistan indicates that the total number of deaths in and around Afghanistan in the Operation Enduring Freedom is 1,030. If we apply the casualty factor, this give us a total of 43.26 casualties due to fuel resupply, and 35.02 due to water resupply. Unfortunately, these casualty numbers are only likely to increase if we pay attention to the information provided by the United Nations report [6].

By reducing the fuel consumption it is possible to reduce the number of fuel resupply convoys and that will reduce the number casualties. Today, there is an increasing number of initiatives being taken by the U.S. DoD in order to reduce the need for fuel in domestic bases as well as those in war situations like Afghanistan. It is also important to highlight that by reducing the number of fuel supply convoys, the forces that are in charge of that task would be free to join other forces committed to other purposes. So, the resupply issue is not only about saving lives (the most important matter) and money, it is also about the opportunity cost.

The U.S. high dependence on oil has environmental and economic consequences, and also affects national security. Talking about this the possibility has to be taken into account that other countries may use the "oil weapon" to stop supplying the U.S. Another important issue is the fact that the global oil market is highly vulnerable to supply disruption since the main oil reserves are concentrated in a quite small area. These two situations do not really depend directly on the U.S., but the fact that military installations in the U.S. depend on the national grid does. This makes military installations really vulnerable to any disruption in the national grid. According to the already-mentioned report "More Fighting – Less Fuel" [7] there are four sources of risk for grid outrages, and they are: overload, and overload was what caused the northeast blackout of 2003. The second source of risk comes from natural disasters and includes hurricanes, tornadoes, electrical storms or other extreme weather events. The third risk that they consider involves sabotage or terrorist activity, whether local, trans-national or state-sponsored, and it includes both conventional and nuclear attacks. The last one comes from cyber attacks since U.S. grid control systems are continuously probed electronically.

Many of the situations that we have described could be improved or even solved by using renewable energies.

3. Possible renewable energy solutions

The renewable energies are becoming more and more important now-a-days. The hydroelectric power is used for a long time, as well as the wind power, earlier as a direct application (like mills) and in the recent days also for generating electrical power. The wave-, tidal-, solar-, biomass-, geothermal- and ocean thermal energies are relatively new type of energy, but the climate change, global warming and their causes and consequences make them very important. From the viewpoint of the military forces not all of them are real solution for the energy supply of a military basis in a foreign country.

According to the geographical possibilities in Afghanistan the following types of renewable energies can be applied: micro hydropower, wind, solar and geothermal energies, and biogas. Among these ones, solar energy is considered to be the most important source since in Afghanistan there are nearly 300 sunny days a year and the solar radiation averages about 6.5 kilowatt-hours per square meter per day [8].

Biogas or biofuels could be used and in fact, the U.S. Power Surety Task Force has already tried to provide forward operating bases with biofuel by means of their Tactical Garbage To Energy Refinery (TGER), a trailer mounted system that converts field waste (paper, plastic, packaging and food waste) into electricity using a standard 60kW diesel generator. Two TGER were deployed to Iraq for a capability demonstration, but they did not perform as well as they had when they were tested in a controlled environment, so further research would be needed.

Wind energy represents a great problem for the bases: the height of the windmills makes them an easy target for enemy forces because, although they would be within the base perimeter, their height is much higher than that of the wall that typically surrounds the bases.

As for geothermal energy in Afghanistan, active geothermal systems are located in the area of the Hindu Kush. There are many low to medium temperature geothermal resources all over Afghanistan. These geothermal fields are mainly water-dominated and can be found in the following areas: Harirud-Badakhshan and Helmand-Arghandab. In principle, bases placed along these areas could take advantage of geothermal energy, either to produce energy or for heating. Geothermal energy for electricity generation needs deep drilling in order to recover water from the deep underground reservoirs, and a geothermal power plant needs to be built. Depending on a power plant during war time is not reliable since the power plant would be an easy target for the enemy forces, so we should discard electricity generation using geothermal energy.

Another possibility concerning geothermal energy is the use of geothermal heat pumps for cooling and heating. They do not need fractured rock and water as occurs in the case of electricity generation. Geothermal Heat Pumps use pipes buried under areas around the building that wants to be heated or cooled either horizontally or vertically in a continuous loop. These pipes must be buried at depths of about 3 meters to 90 meters, so their potential use in war situations could be considered since in the case of the horizontal loop there is no need of digging too deeply.

The most appropriate solution is the installation of devices related to solar power. Solar energy does not only deal with electricity generation but, like geothermal energy, it can also be used for heating.

Solar panels can be installed on the base's roof or inside the perimeter without being a threat since they would be within the perimeter fence and height. They are easy to transport and, in case the base needs to be moved, they can be dismantled and set up again in the new

location. Related to this fact, the Defense Advanced Research Projects Agency (DARPA) has selected Ascent Solar Technologies Inc. for the creation of low-cost lightweight portable photovoltaic that should be able to stand up to battle conditions and environmental extremes. This is a step forward in the future use of solar energy technologies. The use of active systems to provide bases with heating or cooling should be also considered. As well, applications that deal with solar water heating could be applied since, as we saw in the solar energy section, they just need to be mounted on a roof.

4. Conclusions

Climatic change and global warming are facts and any steps taking towards their mitigation should be considered as positives. We have studied the current situation of the U.S. military forces and their domestic oil use as well as their consumption in war situations. Despite the number of initiatives that there are, it is important not only that these initiatives come true but also that military forces become aware of the importance that the good use of energy and renewable energies have, especially because the use of renewable energies can help to decrease the number of casualties in war situations. As many times in history, it is very likely that those devices that are being tested in war cases or that have already been proved would have an application in people's everyday life as happened, for instance, with the Internet. Taken into consideration that the investment on research that many military forces are making is positive since that investment would not only be useful in a war theater or even to win a war, but it is to improve our energy use and general environmental situation.

We have focused on the U.S. military, but renewable solutions could be used by any country with the suitable renewable sources. Maybe other countries cannot make the capital investment that the U.S. can do on new solutions and technologies, but it is true that even if they cannot afford that, they can contribute to their own economy, national security, and environment by starting to use existing green solutions.

To apply of renewable energies can reduce the number of fuel resupply convoys and that will reduce the number casualties, and hopefully it will reduce the number of lost lives.

References

[1] North Atlantic Treaty Organization, *NATO's role in Afghanistan*, http://www.nato.int/ cps/en/natolive/topics_8189.htm, June 22nd, 2010.

[2] U.S. Energy Information Administration, *Petroleum Basic Statistics*, http://www.eia.doe.gov/ basics/quickoil.html, 2008.

[3] U.S. Energy Information Administration, *Country Energy Profiles*, http://www.eia.doe.gov/ country/index.cfm, 2008.

[4] Deloitte, *Energy Security, America's Best Defense*, 2009. http://www.Deloitte.Com/ assets/Dcom-UnitedStates/Local%20Assets/Documents/AD/us_ad_EnergySecurity052010 .pdf, 2010

[5] United Nations Security Council. *Report of the Secretary-General pursuant to paragraph 40 of resolution 1917(2010)*, http://unama.unmissions.org/Portals/UNAMA/SG%20Reports/ June182010_SG_Report.pdf, 2010.

[6] AEPI Report, *Sustain the Mission Project: Casualty Factors for Fuel and Water Resupply Convoys*, http://www.aepi.army.mil/docs/whatsnew/SMP_Casualty_Cost_Factors_Final1-09.pdf Final Technical Report, September 2009.

[7] U.S. Department of Defense, Report of the Defense Science Board Task Force on DoD Energy Strategy, *More Fight –Less Fuel*, http://www.climateaction project.com/docs/Defense_Science_Board_report_Feb_2008.pdf, February 2008.

[8] Asian Development Bank. *Technical Assistance to the Islamic Republic of Afghanistan for Poverty Reduction and Rural Renewable Energy Development*, Financed by the Poverty Reduction Cooperation Fund., http://www.adb.org/ Documents/TARs/AFG/tar-afg-38044.pdf December 2004.